Digital Rights and Safety Handbook

Digital Rights Nepal

Digital Rights and Safety Handbook

Contributors:
Bhola Nath Dhungana
Rukamanee Maharjan
Nikesh Balami
Ananda Gautam
Saurav Bhattarai

Edited by:
Advocate Santosh Sigdel

Curriculum Design Lead:
Tanka Raj Aryal

Published by:
Digital Rights Nepal (DRN)
June 2024

In Collaboration with:
Nepal-U.S. Alumni Network (NUSAN)

Supported by:
US Embassy in Kathmandu under Alumni Engagement Innovation Fund 2023

Disclaimer: The organizations supporting the publication of this resource book do not endorse or take responsibility for any information or opinions expressed within the book. The publisher alone is responsible for the content, and the views and opinions expressed therein do not necessarily reflect those of the supporting organizations.

About the Handbook

Digital Rights and Safety handbook is developed under the Digital Rights School (DRS) Project. This project is a pioneering initiative by Digital Rights Nepal (DRN), in collaboration with the Nepal-U.S. Alumni Network (NUSAN), and supported by the US Embassy in Kathmandu under Alumni Engagement Innovation Fund 2023. The project aims to empower youth with essential digital literacy skills, promote safe online practices, and raise awareness about digital rights and responsibilities. Through a series of workshops and training sessions held across various provinces in Nepal, the DRS project seeks to build a network of informed and proactive digital citizens who can advocate for and protect digital rights in their communities.

The workshops cover a wide range of topics, including online freedom of expression, privacy and data protection, digital safety measures, and the implications of artificial intelligence on digital rights. By providing participants with comprehensive knowledge and practical skills, the DRS project endeavors to foster a more secure, inclusive, and rights-respecting digital environment in Nepal.

This resource book is a foundational tool for Digital Rights Schools, offering in-depth insights and practical guidance on the key aspects of digital rights. It is designed to support the educational efforts of the project and to serve as a lasting reference for participants and stakeholders involved in the digital rights movement in Nepal.

Acknowledgement

We extend our deepest gratitude to all those who have contributed to the creation of this resource book for the Digital Rights School (DRS) project. This book would not have been possible without the unwavering support and collaboration of our esteemed partners, the Nepal-U.S. Alumni Network (NUSAN) and the US Embassy in Kathmandu under Alumni Engagement Innovation Fund 2023. Their generous backing and invaluable input have been instrumental in bringing this project to fruition.

Our heartfelt thanks go to the dedicated team of experts, drafters, and volunteers who meticulously developed and compiled this resource book. We would like to thank Advocate Bhola Nath Dhugana, Ms. Rukamanee Maharjan, Mr. Nikesh Balami, Mr. Ananda Gautam and Mr. Saurav Bhattarai for their hard work, expertise, and commitment in creating a comprehensive guide that will serve as a vital tool for promoting digital rights across Nepal. Similarly, we would like to acknowledge the role played by Mr. Tanka Raj Aryal, Chairperson, DRN, as Curriculum Design Lead and invaluable input provided by Mr. Saroj Bista, Immediate Past President, NUSAN, in finalizing the resource book

We also acknowledge the valuable contributions of the Digital Rights Nepal team, whose efforts in coordinating and managing the project have been exceptional. Their dedication and hard work have ensured that this resource book meets the highest standards of quality and relevance.

Lastly, we thank all the participants and community members whose enthusiasm and commitment drive the success of this initiative. Together, we are fostering a safer, more informed, and empowered digital society.

Santosh Sigdel
Executive Director, Digital Rights Nepal
Coordinator, Nepal Digital Rights School 2024

Table of Content

Chapter 1: Background **1**

A. Overview of Digital Rights 1

B. Importance of Digital Rights in the Digital Age 1

C. Scope and Structure of the Resource Book 2

Chapter 2: Understanding of Digital Rights **4**

A. Conceptual Framework of Digital Rights 4

B. Digital Right Principles 5

C. Historical Evolution of Digital Rights 7

D. International Legal Instruments and Declarations Relating to Digital Rights 10

Chapter 3: Online Freedom of Expression **13**

A. Freedom of Expression 13

B. Principles of Freedom of Expression in the Digital Sphere 16

C. Challenges and Threats to Online Freedom of Expression 18

D. Case Studies and Examples 21

Chapter 4: Privacy and Data Protection **24**

A. Introduction 24

B. Principles of Privacy and Data Protection 25

C. Legal Frameworks for Privacy Protection 27

D. Emerging Challenges in Privacy and Data Protection 30

Chapter 5: Information Integrity **32**

A. Importance of Information Integrity in the Digital Era 32

B. Disinformation, Misinformation, and Fake News 33

C. Strategies for Promoting Information Integrity Online 34

Chapter 6: Internet Governance **36**

A. Evolution and History of Internet Governance 36

B. Multi-Stakeholder Approach to Internet Governance 37

C. Role of Governments, Civil Society, and Private Sector in Internet Governance 39

Chapter 7: Digital Safety Measures **42**

A. Threat Landscape in the Digital Environment 42

B. Best Practices for Digital Safety 45

C. Digital Rights Vis-a-Vis Digital Safety 50

Chapter 8: AI and Digital Rights 51

A. Background 51

B. Implications of Artificial Intelligence on Digital Rights 53

C. Ethical Considerations in AI Development and Deployment 54

D. Regulatory Frameworks for AI and Digital Rights Protection 55

Chapter 9: Digital Literacy/Inclusion 58

A. Importance of Digital Literacy in Promoting Digital Rights 58

B. Strategies for Promoting Digital Inclusion 59

C. Addressing Barriers to Digital Literacy and Inclusion 61

Chapter 10: E-Governance / Services 63

A. Background 63

B. Emergence of e-Governance Concept 65

C. Guiding Principles and Scope of e-Governance 66

D. Issues and Challenges 68

Chapter 11: Internet and Crime 71

A. Overview of Cybercrime and Its Impact on Digital Rights 71

B. Legal Responses to Cybercrime 74

C. Collaboration and Cooperation in Combating Cybercrime 77

Chapter 12: Support/Grievance Mechanisms to address online violence 80

A. Importance of Support and Grievance Mechanisms 80

B. Role of Civil Society and Advocacy Groups 82

C. Governmental and Non-Governmental Support Services 83

Chapter 13: Digital Wellbeing 85

A. Impacts of Digital Technologies in Wellbeing 85

B. Strategies for Promoting Digital Wellbeing 86

C. Support Services Available for Digital Wellbeing 87

D. Digital Tools for Digital Wellbeing 88

Chapter 1
Background

A. Overview of Digital Rights

Digital rights are the human rights and legal protections that individuals have in the digital realm. These rights are an extension of fundamental human rights such as freedom of expression, privacy, and access to information, adapted to the digital age. Digital rights encompass various issues including online freedom of expression, privacy and data protection, access to information, digital safety, and more. They ensure that individuals can safely and freely navigate the internet, participate in online activities, and utilize digital technologies without fear of undue restriction or harm.

B. Importance of Digital Rights in the Digital Age

In today’s interconnected world, digital rights have become increasingly crucial. The rapid advancement of technology has transformed how we communicate, access information, and engage in social, political, and economic activities. The importance of digital rights can be summarized as follows:

- Protection of Personal Freedoms: Digital rights protect individual freedoms such as freedom of expression, privacy, and the right to access information. These rights are fundamental to democratic societies and the free flow of ideas.

- Privacy and Data Security: With the vast amounts of personal data being collected and processed online, digital rights ensure that individuals' privacy is respected and that data protection measures are in place to secure sensitive information.

- Access to Information and Services: Digital rights guarantee equitable access to information and digital services, which is essential for education, employment, healthcare, and civic participation.
- Empowerment and Inclusion: By promoting digital literacy and inclusion, digital rights empower individuals to participate fully in the digital society, bridging the digital divide and ensuring that everyone benefits from technological advancements.
- Combating Misinformation and Abuse: Digital rights help address issues of misinformation, cyberbullying, and other forms of online abuse, creating a safer and more trustworthy digital environment.

C. Scope and Structure of the Resource Book

This resource book is designed to provide a comprehensive understanding of digital rights and their various facets, aiming to equip readers with the knowledge and tools necessary to navigate the digital world safely and responsibly. It is structured to cover a wide range of topics, offering in-depth insights and practical guidance.

The book begins with Chapter 1 “Background”, which introduces the fundamental concepts of digital rights, their importance in the modern digital age, and their historical evolution. Chapter 2 "Understanding of Digital Rights,” lays the foundation by exploring the conceptual framework, historical evolution, and international legal instruments related to digital rights. Chapter 3 "Online Freedom of Expression," discusses the principles, challenges, and case studies related to maintaining freedom of expression in the digital sphere. Following this, Chapter 4 "Privacy and Data

Protection," examines the principles, legal frameworks, and emerging issues in protecting privacy and data online.

Subsequent chapters delve into specific areas of concern and interest. Chapter 5, "Information Integrity," highlights the importance of information integrity, addressing issues like disinformation and strategies for promoting accuracy online. Chapter 6, "Internet Governance" provides an overview of internet governance models and the roles of various stakeholders. Chapter 7 "Digital Safety Measures," focuses on the digital threat landscape and best practices for ensuring safety online.

The book also explores advanced topics such as the implications of artificial intelligence on digital rights in Chapter 8, and the importance of digital literacy and strategies for promoting digital inclusion in Chapter 9. Chapter 10 "E-Governance/Services" discusses the role of e-governance in promoting digital rights, while Chapter 11 reviews cybercrime issues and responses. Chapter 12, "Support/Grievance Mechanisms to Address Online Violence," examines support mechanisms for online violence, and Chapter 13, "Digital Wellbeing," looks at the impact of digital technologies on well-being and strategies for promoting digital health.

This resource book aims to be a valuable tool for individuals, educators, policymakers, and advocates, providing the knowledge and resources needed to protect and promote digital rights.

Chapter 2

Understanding of Digital Rights

A. Conceptual Framework of Digital Rights

Human rights are the set of rights of every individual as outlined by the international human rights instruments. Universality and inalienability, interdependent and indivisible, equal and non-discrimination are some of the fundamental principles of human rights. The list of human rights can be outlined under different categories of civil, political, economic, social and cultural rights, and so on.

The country's constitutions further reiterate and express commitments towards international human rights standards by incorporating those rights as fundamental rights to implement in the local context effectively. The Constitution of Nepal guarantees thirty-one different types of rights as fundamental rights[1] which are equally applicable both online and offline.

We live in a world today where information and communication technology (ICT) or digital technologies are rapidly growing. The digital infrastructure provides online services for everything from social media to e-commerce, virtual collaboration to e-learning, government service delivery to payment systems, and social connectivity to each other.

This increasingly pervasive, unpredictable and rapidly changing interaction between ICT and society brings with it a wide range of new human rights risks and ethical dilemmas for companies in the ICT industry, especially for how to

[1] See Part 3 (Art. 16-46) of the Constitution of Nepal.

protect and advance freedom of expression and privacy online.[2] As human rights apply both online and offline, digital technologies provide new means to exercise human rights. These new means or platforms of exercising human rights exposes both the opportunities and the challenges. Data protection and privacy, digital identity, the use of surveillance technologies, online violence, and harassment are of particular concern.[3]

As with the application of human rights provisions in the offline world, the rights of the people to access, use, create, and publish digital media and also the right to access and use computers, any electronic devices, internet, and telecommunications can be defined as digital rights. Thus, digital rights imply the elaboration of human rights in the internet era.

Digital rights are interchangeably referred to as internet rights, internet freedom, net freedom, digital freedom, cyber rights, etc. as well.

B. Digital Right Principles

As described above, digital rights are the elaboration of human rights in the internet era, and the fundamental principles of human rights such as universality, inalienability, and indivisibility are equally applicable in the digital rights concepts as well. It is therefore essential that all actors of the public and private sector must respect and protect human rights on the internet.

All fundamental principles that apply in the general human rights world apply online too. To realize the same vision of rights-based internet environment, the Internet Rights and Principles Dynamic Coalition and UN Internet Governance

[2] https://www.bsr.org/reports/BSR_Protecting_Human_Rights_in_the_Digital_Age.pdf

[3] https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Digital_Human_Rights_Summary_PDF.pdf

Forum jointly crafted "the Charter of Human Rights and Principles for the Internet", which outlines the following 10 Internet rights and principles[4]:

1. ***Universality and Equality:***

   All humans are born free and equal in dignity and rights, which must be respected, protected and fulfilled in the online environment.

2. ***Rights and Social Justice:***

   The Internet is a space for the promotion, protection, and fulfillment of human rights and the advancement of social justice. Everyone must respect the human rights of others in the online environment.

3. ***Accessibility:***

   Everyone has an equal right to access and use a secure and open Internet.

4. ***Expression and Association:***

   Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural, or other purposes.

5. ***Privacy and Data Protection:***

   Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal, and disclosure.

[4] Internet Rights and Principles Dynamic Coalition UN Internet Governance Forum can be accessed at https://internetrightsandprinciples.org/

6. *Life, Liberty, and Security:*

The rights to life, liberty, and security must be respected, protected, and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.

7. *Diversity:*

Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate a plurality of expression.

8. *Network Equality:*

Everyone shall have universal and open access to the Internet's content, free from discriminatory prioritization, filtering, or traffic control on commercial, political, or other grounds.

9. *Standards and Regulation:*

The Internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion, and equal opportunity for all.

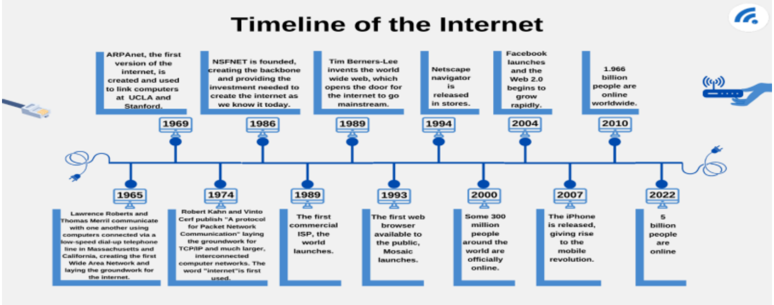
10. *Governance:*

Human rights and social justice must form the legal and normative foundations upon which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation, and accountability.

C. Historical Evolution of Digital Rights

The idea of digital rights is linked with the development of the internet. The history of the internet can be traced back to the decade of the 1950s, when it was primarily imagined, developed, and used for defense purposes. The first decentralized system was the Arpanet, a project of the

Advanced Research Projects Agency (ARPA) under the US Department of Defense, which connected the computers of the four universities in the US.[5] The following picture gives a glimpse of the history of the internet:

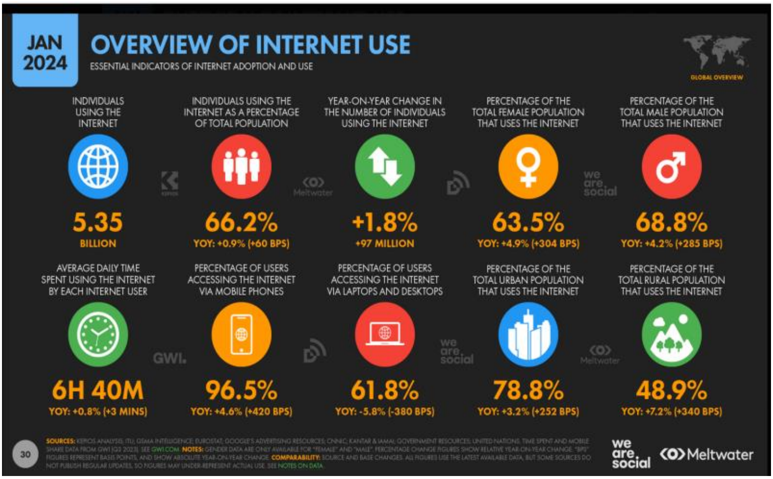

Timeline of the Internet
1969
ARPAnet, the first version of the internet, is created and used to link computers at UCLA and Stanford.
1986
NSFNET is founded, creating the backbone and providing the investment needed to create the internet as we know it today.
1989
Tim Berners-Lee invents the world wide web, which opens the door for the internet to go mainstream.
1994
Netscape navigator is released in stores.
2004
Facebook launches and the Web 2.0 begins to grow rapidly.
2010
1.966 billion people are online worldwide.
1965
Lawrence Roberts and Thomas Merril communicate with one another using computers connected via a low-speed dial-up telephone line in Massachusetts and California, creating the first Wide Area Network and laying the groundwork for the internet.
1974
Robert Kahn and Vinto Cerf publish "A protocol for Packet Network Communication" laying the groundwork for TCP/IP and much larger, interconnected computer networks. The word "internet"is first used.
1989
The first commercial ISP, the world launches.
1993
The first web browser available to the public, Mosaic launches.
2000
Some 300 million people around the world are officially online.
2007
The iPhone is released, giving rise to the mobile revolution.
2022
5 billion people are online

Source: broadbandsearch.net

The use of the internet is rapidly growing from education to e-commerce, online training to online shopping, and online payment to digital banking. Most aspects of our lives are dependent in some form or another on the Internet, including our economic and financial systems, social interactions, education, work, and civic participation, as well as the many services we use to complement our lives, from entertainment and banking services to booking travel. The government's policy also emphasizes the digitalization of its services, which impact the common people. In this way in many aspects, the internet has become indispensable to aspects of modern life.

This info-graph highlights the current trend of internet usage around the world:

[5] Wade Hostel and David Nonhoff (2019) Internet Governance: Past, Present and Future. Konrad-Adenauer-Stiftung e. V.. Also *See*, Bygrave, L. A., Bing, J. (2009). Internet Governance: Infrastructure and Institutions. Oxford University Press.



JAN 2024

OVERVIEW OF INTERNET USE

ESSENTIAL INDICATORS OF INTERNET ADOPTION AND USE

GLOBAL OVERVIEW

INDIVIDUALS USING THE INTERNET: 5.35 BILLION

INDIVIDUALS USING THE INTERNET AS A PERCENTAGE OF TOTAL POPULATION: 66.2% YOY: +0.9% (+60 BPS)

YEAR-ON-YEAR CHANGE IN THE NUMBER OF INDIVIDUALS USING THE INTERNET: +1.8% +97 MILLION

PERCENTAGE OF THE TOTAL FEMALE POPULATION THAT USES THE INTERNET: 63.5% YOY: +4.9% (+304 BPS)

PERCENTAGE OF THE TOTAL MALE POPULATION THAT USES THE INTERNET: 68.8% YOY: +4.2% (+285 BPS)

AVERAGE DAILY TIME SPENT USING THE INTERNET BY EACH INTERNET USER: 6H 40M YOY: +0.8% (+3 MINS)

PERCENTAGE OF USERS ACCESSING THE INTERNET VIA MOBILE PHONES: 96.5% YOY: +4.6% (+420 BPS)

PERCENTAGE OF USERS ACCESSING THE INTERNET VIA LAPTOPS AND DESKTOPS: 61.8% YOY: -5.8% (-380 BPS)

PERCENTAGE OF THE TOTAL URBAN POPULATION THAT USES THE INTERNET: 78.8% YOY: +3.2% (+252 BPS)

PERCENTAGE OF THE TOTAL RURAL POPULATION THAT USES THE INTERNET: 48.9% YOY: +7.2% (+340 BPS)

30

SOURCES: KEPIOS ANALYSIS; ITU; GSMA INTELLIGENCE; EUROSTAT; GOOGLE'S ADVERTISING RESOURCES; CNNIC; KANTAR & IAMAI; GOVERNMENT RESOURCES; UNITED NATIONS. TIME SPENT AND MOBILE SHARE DATA FROM GWI (Q3 2023). SEE GWI.COM. NOTES: GENDER DATA ARE ONLY AVAILABLE FOR "FEMALE" AND "MALE". PERCENTAGE CHANGE FIGURES SHOW RELATIVE YEAR-ON-YEAR CHANGE. "BPS" FIGURES REPRESENT BASIS POINTS, AND SHOW ABSOLUTE YEAR-ON-YEAR CHANGE. COMPARABILITY: SOURCE AND BASE CHANGES. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCES DO NOT PUBLISH REGULAR UPDATES, SO FIGURES MAY UNDER-REPRESENT ACTUAL USE. SEE NOTES ON DATA.

we are social   Meltwater

In the context of Nepal also, the use of the internet has become an integrated part of lifestyle from communication, expression of opinion, shopping, payment, service delivery, record keeping, data management, etc.

Following is the latest data, which describes internet penetration in Nepal.

Market Proportion of Data Service

Broadband Services	Number of Subscription	Market Proportion (%)
Fixed Broadband (Wired)	14236000	33.62
Fixed Broadband (Wireless)	44185	0.10
Mobile Broadband	28063188	66.28
Total Broadband Service	42343373	100

Source: Telecommunication Indicators Chaitra, 2080 (March 14– April 12, 2024), Nepal Telecommunication Authority, Published in Baishakh 2081

The evolution, design, and governance of the internet have significant social, political, and economic implications that affect the rights of users around the world. The decisions that shape the internet and digital platforms can both advance and restrict how users communicate and how information is accessed and shared, thus having a significant effect on how the internet can impact the public interest, especially in regard to social justice, civil liberties, and human rights.

Over the last few decades, both governmental and civil society actors have been working to define the relationship between human rights and the Internet on a national and international level.

D. International Legal Instruments and Declarations Relating to Digital Rights

The human rights instruments applied offline must also protect human rights online. The Universal Declaration of the Human Rights 1948 is one of the key instruments relating to digital rights. Article 12 of the Declaration protects against arbitrary interference against privacy, whereas 19 affirms the rights to freedom of opinion and expression.

Similarly, International Covenant on Civil and Political Rights (ICCPR) guarantees the freedom of expression equally in both online and offline platforms. Article 19(2) states that "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.[6] Article 17 of the Covenant imposes legally binding obligations for the member states to protect and guarantee right to privacy.

Similarly, the Ronvention on the Rights of the Children (CRC), 1989 Addresses the rights of children in the digital age, including their protection and participation online. Article 16 of the Convention mandates protection against arbitrary interference with privacy, whereas Article 17 ensures access to information and media.

[6] International Covenant on Civil and Political Rigths (ICCPR) Article 19 (2)

Further efforts have been initiated through the different forums and instruments more particularly focusing on assurance of digital rights. In 2005, the Tunis Agenda for the Information Society stated that “measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.[7]

Similarly, in 2012, the UN Human Rights Council adopted a key resolution on the promotion, protection, and enjoyment of human rights on the Internet, affirming that “the same rights that people have offline must also be protected online.[8]” A similar level of commitment was also extended by the UN Human Rights Council in 2016, which states that “[T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.”[9]

To provide a recognizable framework anchored in international human rights for upholding and advancing human rights in the online environment, the Internet Rights and Principle Dynamic Coalition introduced "The Charter of Human Rights and Principles for the Internet" in 2014 under the initiation of the UN Internet Governance Forum. The

[7] See, Tunis Agenda for Information Society, World Summit on Information Society, Geneva 2023- Tunis 2005. WSIS-05/TUNIS/DOC/6(Rev.1)-E 18 November 2005

[8] The resolutions and decisions adopted by the Human Rights Council will be contained in the report of the Council on its twentieth session (A/HRC/20/2), chap. I.

[9] The Resolutions on the promotion, protection and enjoyment of human rights on the internet’, A/HRC/32/L.20 (2016) at para 1

Charter highlights 10 different internet rights and principles, which have been covered above.[10]

The Budapest Convention on Cybercrime – 2001 is the first international treaty seeking to address internet and computer crime by harmonizing national laws. The convention defines various forms of cybercrime, and facilitates international cooperation in cybercrime investigations. The government of Nepal has principally agreed to assess the Budapest Convention, however official adoption has not taken place.

[10] For detail, see, August 2014 – 4th Edition Internet Rights and Principles Dynamic Coalition UN Internet Governance Forum which can be accessed at https://internetrightsandprinciples.org/

Chapter 3
Online Freedom of Expression

A. Freedom of Expression

Freedom of expression is a fundamental right that allows people to express themselves and their ideas without fear of punishment or censorship.[11] This right includes freedom to seek, receive, and impart all kinds of information and ideas, regardless of frontiers, through any media including orally, in writing or print, and the form of art.[12] The normative content and scope of freedom of opinion and expression that includes, among others, freedom to hold opinions; freedom to impart information and ideas; freedom to receive information and ideas; and access to information.[13]

Freedom of Expression in a day-to-day life[14]

- When you share your views or seek out information, online or offline, you're exercising your right to freedom of expression.
- When you criticize your government for not living up to its promises, you're exercising your right to freedom of expression.
- When you question or debate religious, political, social, or cultural practices, you're exercising your right to

[11] See John Steel & Julian Petley (Eds.). (2024). *The Routledge Companion to Freedom of Expression and Censorship.* Routledge.

[12] Article 19(2), International Covenant on Civil and Political Rights 1966.

[13] See United Nations Human Rights Committee. (12 September 2011). General Comment No. 34 - Article 19: Freedom of Opinion and Expression.

[14] This section is based on materials published by Article 19, available at https://www.article19.org/what-is-freedom-of-expression/ (accessed on 29 April 2024).

freedom of expression.

- When you attend a peaceful protest or organize one, you're exercising your right to freedom of expression.
- When you create a work of art, you're exercising your right to freedom of expression.
- When you comment on a news article – whether you're supporting it or criticizing it – you're exercising your right to freedom of expression.

It is enshrined in various international human rights instruments including Article 19 of the Universal Declaration of Human Rights 1948 and Article 19 of the International Covenant on Civil and Political Rights 1966.

It sets indispensable conditions for the full development of the person.[15] It enables individuals to achieve self-fulfillment and to meaningfully participate in decision-making and political affairs.[16] It is crucial for a healthy democracy, allowing for open debate, the exchange of ideas, and criticism of government and power.[17] It helps ensure that governments are accountable and that people can participate in shaping their societies, through questioning and debate that lead to better policies and more stable societies.[18]

It should be noted that freedom of expression is not an absolute right. It can be limited in certain circumstances, namely protection of rights or reputations of others;

[15] United Nations Human Rights Committee. (12 September 2011). General Comment No. 34 - Article 19: Freedom of Opinion and Expression. Para 2.

[16] United Nations Human Rights Committee. (12 September 2011). General Comment No. 34 - Article 19: Freedom of Opinion and Expression. Para 2.

[17] Article 19. (n.d.). What is freedom of expression? (0nline content). Available at https://www.article19.org/what-is-freedom-of-expression/ (accessed on 29 April 2024).

[18] Article 19. (n.d.). What is freedom of expression? (0nline content). Available at https://www.article19.org/what-is-freedom-of-expression/ (accessed on 29 April 2024).

protection of national security or public order; and public health or morals.[19] To limit this right, a three-part test has been established to determine if a restriction on expression is legitimate.[20]

Three-part test and Limitations of Freedom of Expression[21]

1. Lawful Restrictions: The restriction on expression must be provided by law. It can't be based on arbitrary decisions by officials or the government.

2. Legitimate Aims: The restriction must pursue a legitimate aim. These aims include:

- Respect for the rights or reputations of others: This protects individuals from defamation and harassment.
- Protection of national security or public order: This allows governments to restrict speech that could incite violence or endanger national security.
- Public health or morals: This might be used to restrict hate speech or pornography.

3. Necessity: The restriction must be necessary to achieve the legitimate aim. It should be the least intrusive option available and there should not be other, less restrictive ways to achieve the same goal.

The obligation to respect freedoms of opinion and expression is binding on every State party as a whole i.e. responsibility lies with executive, legislative, and judicial organs of the

[19] Article 19(3), International Covenant on Civil and Political Rights 1966.

[20] United Nations Human Rights Committee. (12 September 2011). General Comment No. 34 - Article 19: Freedom of Opinion and Expression. Para 21-35.

[21] United Nations Human Rights Committee. (12 September 2011). General Comment No. 34 - Article 19: Freedom of Opinion and Expression. Para 21-35.

State and other public or governmental authorities.[22] Equally, this right is so fundamental to each and every one of us – from civil society to journalists, educators, writers, artists, lawyers, and activists – that we all must stand up for it.[23]

B. Principles of Freedom of Expression in the Digital Sphere

The internet is considered to be one of the most powerful tools in facilitating the receiving, sharing, and imparting of information and ideas, instantly, across borders and to wide audiences.[24] It enables individuals to engage with diverse views, perspectives, and to access an array of resources to assist them formulate their own views.[25] It is important to note that the United Nations Human Rights Council has already pronounced and reaffirmed that "the same rights that people have offline must also be protected online, in particular freedom of expression”.[26] Likewise, the Council has adopted the resolution on the promotion, protection, and enjoyment of human rights on the Internet.[27]

[22] OHCHR.(n.d.). General comment No.34 on Article 19: Freedoms of opinion and expression. (online material). Available at https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedoms-opinion-and (accessed on 29 April 2024).

[23] Article 19.(n.d.). What is freedom of expression? (0nline content). Available at https://www.article19.org/what-is-freedom-of-expression/ (accessed on 29 April 2024).

[24] Media Legal Defence Initiative. (n.d.). Training Manual on Digital Rights and Freedom of Expression Online. Available at https://mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf (accessed on 2 May 2024).

[25] Media Legal Defence Initiative. (n.d.). Training Manual on Digital Rights and Freedom of Expression Online. Available at https://mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf (accessed on 2 May 2024).

[26] United Nations Human Rights Council. (June 2012).HRC Resolution 20/8 and United Nations Human Rights Council. (June 2014).HRC Resolution 26/13.

[27] United Nations Human Rights Council. (July 2021).HRC Resolution A/HRC/47/L.22.

In this light, the principles of freedom of expression in the digital space can be presented as follows[28]:

- Online freedom of expression protects information, opinions, and ideas of all kinds disseminated through any media including the Internet, regardless of borders. It includes the right not only to impart but also to seek and receive information in the digital space.
- The Internet is a public good that has become essential for the effective exercise and enjoyment of the right to freedom of expression.
- The exercise of the right to online freedom of expression may be subject to restrictions only on grounds specified by international law, including for the protection of the rights of others such as the protection of privacy, protection from hate speech or copyright.
- No restriction on freedom of expression on the ground of protection of the rights of others may be imposed unless the State can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect those interests. The burden of demonstrating the validity of the restriction rests with the State.
- States must not only refrain from interfering with online freedom of expression but are also under a positive obligation to protect online freedom of expression from interference by private parties.
- Protecting and promoting online expression requires collaboration between governments, platforms, civil

[28] Article 19.(2013). The Right to Share: Principles on Freedom of Expression and Copyright in the Digital Age. PP. 7-9, and Media Legal Defence Initiative. (n.d.). Training Manual on Digital Rights and Freedom of Expression Online. Available at https://mediadefence.org/wp-content/uploads/2020/06/MLDI-Training-Manual-on-Digital-Rights-and-Freedom-of-Expression-Online.pdf (accessed on 2 May 2024).

society organizations, and individual users. Multi-stakeholder approach must be undertaken to protect and promote online freedom of expression.

- The digital sphere should be accessible to everyone, regardless of background or technical expertise. This fosters a more diverse and representative online public discourse.
- Online Platforms and governments should be transparent about their content moderation policies and how they handle user data. There should be clear mechanisms for users to appeal content removal decisions.
- Content moderation efforts by online platforms should be proportionate to the potential harm caused by the content. This avoids unnecessary censorship and ensures freedom of expression is not unduly restricted.
- Freedom of expression needs to be balanced with other important rights, such as privacy, personal data protection, and protection from harm. This includes preventing the spread of hate speech, misinformation, and incitement to violence.

C. Challenges and Threats to Online Freedom of Expression

In 2016, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression pointed out that the challenges and threats to freedom of opinion and expression are severe, such as

- Unnecessary surveillance and threat to individual security online;
- Internet shutdowns;
- Misuse of measures to preventing or countering terrorism and violent extremism; and violation of freedom of expression;

- Undermining right to information;
- Criminalization of criticism;
- Restrictions on expression relating to religion and belief; and
- Singling out of groups such as women.[29]

In this light, key challenges and threats to online freedom of expression are presented as follows:

Government Control and Censorship: Government control and censorship is one of the major challenges and threats to the online freedom of expression. Governments may restrict access to certain websites or content they deem objectionable, limiting access to information and diverse viewpoints, which is called Blocking and Filtering.

The governments around the world are proposing new laws and regulations to regulate the online space and issues like hate speech, defamation, disinformation etc. which can be misused to silence dissent on online spaces. Similarly, extensive government surveillance can create an atmosphere of fear, discouraging people from expressing critical opinions.

Content Moderation by Platform: Internet platforms play vital role in promoting online freedom of expression. However, some of their own activities and the way they deal with content generated by users have posed challenges and threats to the exercise of this right. Social media platforms and other online spaces have content moderation policies that can sometimes lead to the removal of legitimate content, even if it doesn't violate the platform's terms. Similarly, the algorithms adopted by the companies for filtering content might be biased, disproportionately removing content from

[29] United Nations General Assembly. (6 September 2016). Promotion and protection of the right to freedom of opinion and expression. A/71/373.

certain groups or viewpoints. Further, the lack of transparency in content moderation decisions by the tech companies makes it difficult for users to understand why content is removed and to challenge those decisions.

Misinformation and Disinformation: In recent years, we hear a lot about the 'fake news'. False or misleading information which are categorized as misinformation, disinformation and mal-information, can spread quickly online, manipulating public opinion and eroding trust in reliable sources. This will not only raise concern about integrity of the information online but governments may take measures to regulate online information ecosystem which may pose threat to online freedom of expression.

Cyberbullying and Online Harassment: Threats, harassment, and abuse online can silence individuals and create a hostile environment for free expression. This affects vulnerable groups such as women, LGBTIQA++, and marginalized communities.

Protection of journalists and media: It is hard to define and protect journalists and the media in an environment now saturated with bloggers and social media writers, and defend them from online harassment, particularly women who are disproportionately subject to online harms.

Digital Divide: Lack of access to technology and the internet can exclude certain communities from participating in online discourse.

Threats to Anonymity and Privacy: If online anonymity is compromised, it can discourage people from expressing unpopular views for fear of retribution.

D. Case Studies and Examples

- ### Internet Shutdowns in India

  Local authorities in India have shut down the internet 127 times between January 2020 and December 2022, citing reasons like preventing or in response to protests, preventing cheating in exams, in response to communal violence, and other law and order concerns.[30] For instance, in August 2019, the Indian government completely blocked all communication networks in Jammu and Kashmir, including landlines, fixed-line internet, and mobile networks to prevent Kashmiris from organizing protests after the government revoked the state's constitutional autonomous status, splitting it into two separate federally governed territories.[31] While some services were gradually restored, mobile 4G internet access remained effectively down for over 500 days, until February 2021.[32] The shutdown impacted every aspect of daily life; and also severely limited access to information and communication, hindering free expression and peaceful assembly at large.

[30] Human Rights Watch and Internet Freedom Foundation. (2023). "No Internet Means No Work, No Pay, No Food" Internet Shutdowns Deny Access to Basic Rights in "Digital India". Available at https://hrw.org/sites/default/files/media_2023/06/india0623web_1.pdf. (Accessed on 6 May 2024).

[31] Human Rights Watch and Internet Freedom Foundation. (2023). "No Internet Means No Work, No Pay, No Food" Internet Shutdowns Deny Access to Basic Rights in "Digital India". Available at https://hrw.org/sites/default/files/media_2023/06/india0623web_1.pdf. (Accessed on 6 May 2024).

[32] Human Rights Watch and Internet Freedom Foundation. (2023). "No Internet Means No Work, No Pay, No Food" Internet Shutdowns Deny Access to Basic Rights in "Digital India". Available at https://hrw.org/sites/default/files/media_2023/06/india0623web_1.pdf. (Accessed on 6 May 2024).

- ### Tiktok Ban in Nepal

  In November 2023, Nepal banned TikTok, citing its negative impact on "social harmony, family structure, and family relations."[33] Some authorities expressed worry about the spread of hate speech and content deemed disruptive to social order on the platform. This reasoning was criticized for being vague and lacking concrete evidence. The ban affected over 2.2 million Nepali TikTok users, limiting their access to a popular platform for entertainment and self-expression. The ban was challenged in the Supreme Court, highlighting ongoing legal debates about the scope of government authority to regulate online content but the Supreme Court did not provide an "interim order".[34] It should be noted that the ban undermines the freedom of expression of the people and is also in conflict with the constitutional provisions of Nepal.

- ### Social Media Ban in Pakistan

  In Pakistan, social media platforms have been intermittently banned or restricted by the government, citing reasons such as national security, blasphemy, or to curb the spread of misinformation and fake news. One notable instance was in 2020 when the Pakistan Telecommunication Authority (PTA) blocked the popular video-sharing app TikTok multiple times, citing concerns over inappropriate content. Similarly, in 2021,

[33] BBC. (14 November 2023). Nepal bans TikTok citing disruption to social harmony. (Online material). Available at https://www.bbc.com/news/business-67411535. (Accessed on 6 May 2024).

[34] Legal World.Com. (21 November 2023). Nepal SC refuses "interim order" to lift TikTok ban, issues show cause to govt. (Online material). Available at https://legal.economictimes.indiatimes.com/news/international/nepal-sc-refuses-interim-order-to-lift-tiktok-ban-issues-show-cause-to-govt/105394934 (Accessed on 6 May 2024).

access to various social media platforms, including Facebook, Twitter, and YouTube, was temporarily suspended following violent protests. These actions have sparked debates around freedom of expression and the government's control over online content, with critics arguing that such bans infringe upon citizens' rights to access information and express themselves online.

Chapter 4
Privacy and Data Protection

A. Introduction

We share our personal information such as name, age, gender, family details, images, and phone numbers in many places including the digital platform. Moreover, with the emerging dominance of social media, so much of personal information goes to the public even without knowing it.

In the digital world, public and private sectors both have been collecting different data through different digital sources. Telecommunication service providers, bank and financial institutions and payment service operators and providers, utility service providers collect our information while approaching for their service. We provide various personal data to the government authorities in different steps for example in the vital registration process, when obtaining citizenship, passport, driving license. The private sector also collects data during service delivery, the best examples include sharing our numbers and geographical information while using ride-sharing apps, online shopping, food delivery services, etc.

Data has a wide meaning. It not only includes formal statistics collected, archived, and disclosed through formal governmental or non-governmental channels but also personal information. The Statistics Act, 2079 (2022) of Nepal defines data as archival or information about details of economic, social, physical, and environmental circumstances[35] which also incorporates systematic

[35] Statistics Act, 2079 Sec. 2 (e).

collection, presentation, and analysis. Personal information also falls under the wider definition of data.

The Privacy Act, 2075 (2018) of Nepal broadly defines personal information under Sec. 2 (c). It encompasses various types of information related to an individual, including their caste, ethnicity, birth, origin, religion, color, marital status, educational qualifications, and contact details (address, telephone, email). It also includes identification documents such as passports, citizenship certificates, national identity cards, driving licenses, and voter identity cards. Personal correspondence, biometric data (like thumb impressions, fingerprints, retina scans, and blood groups), criminal history, and professional or expert opinions expressed during decision-making processes are also considered personal information under this Act.

The protection of data, especially personal information, whether it pertains to individuals or institutions such as companies, firms, or organizations, is crucial. Establishing a legal mechanism for data protection is essential, and privacy should be the core focus in the arrangement of such mechanisms.

B. Principles of Privacy and Data Protection

Privacy and data protection are prominent topics of global concern today. Nations and regions are establishing various legal measures to address these issues. The Organization for Economic Cooperation and Development (OECD) was the first organization to endorse principles of privacy protection, through the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which recognize both the need for and the risks of facilitating transborder data flows.[36] The European Union (EU) officially enacted the General Data Protection Regulation in 2016.[37] The EU even emphasizes that the transfer of personal data to a third country should be permitted only when the third country in question ensures an adequate level of protection.[38]

Different principles are considered as guiding frameworks in formulation and enforcement of privacy and data protection policies. The OECD Guidelines promote eight principles, applicable in both the public and the private sector, which countries should respect in developing their privacy protection frameworks: (i) collection limitation; (ii) data quality; (iii) purpose specification; (iv) use limitation; (v) security safeguards; (vi) openness; (vii) individual participation; and (viii) accountability.

Similarly, The Asia-Pacific Economic Cooperation (APEC) framework endorses the following principles: (i) preventing harm; (ii) notice; (iii) collection limitations; (iv) use of personal information; (v) choice; (vi) integrity of personal information; (vii) security safeguards; (viii) access and correction; and (ix) accountability.[39]

The Charter of the Organization of American States outlined Updated Principles on Privacy and Personal Data Protection,[40] those are 1. Lawful Purposes and Loyalty, 2. Transparency and Consent, 3. Relevance and Necessity, 4.

[36] https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf?expires=1717228253&id=id&accname=guest&checksum=81356C31428C9303C23CAC87866B9822 Accessed on 05 May 2024.

[37] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

[38] Directive 95/46/EC, recitals 1

[39] APEC Privacy Framework (2015) https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 Accessed on 05 June 2024

[40] Organization of American States Department of International Law Secretariat for Legal Affairs

Limited Processing and Retention, 5. Confidentiality, 6. Security of Data, 7. Accuracy of Data, 8. Access, Rectification, Erasure, Objection and Portability, 9. Sensitive Personal Data, 10. Accountability, 11. Trans-Border Flow of Data and Accountability, 12. Any exception to whichever one of these Principles should be provided for expressly and specifically in domestic law, be made known to the public, and 13. Data Protection Authorities.

C. Legal Frameworks for Privacy Protection

The right to privacy is established in international law and regarded as a fundamental human right. The core privacy principles are laid down in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights which guarantee the protection of the privacy of every individual in their personal sphere both offline and online.

Over the past few decades, the domestic and international framework for privacy has been expanded. In comparison to this, no such specific international legal framework is developed with specific obligations in the domain of privacy and data protection. The EU has developed a regional mandatory legal framework, General Data Protection Regulation (GDPR), and some international organizations like OECD and AEPC have endorsed principles but globally applicable instruments are yet to be developed.

In Nepal, there is no specific law that addresses data protection regulation. But, can be traced to scattered provisions contained in other laws along with the Constitution.

Constitutional of Nepal

The Constitution of Nepal promulgated in 2072 (2015) guarantees privacy as fundamental rights. Article 28 of the Constitution states that the privacy of any person, his or her residence, property, document, data, correspondence, and matters relating to his or her character shall, except in accordance with law, be inviolable. Previous Constitutions the Constitution of the Kingdom of Nepal, 2047[41] and the Interim Constitution of Nepal 2063[42] also recognized privacy as fundamental rights.

The Privacy Act, 2075

In order to enforce the prevalent provisions related to right to privacy under the Constitution of Nepal, the parliament enacted the Privacy Act, 2075 (2018). The objectives of the Act are to ensure the right to privacy of the matters relating to body, residence, property, document, data, correspondence and character of every person, to manage the protection and safe use of personal information remained in any public body or institution, and to prevent encroachment on the privacy of every person.[43] The Act covers the rights to privacy for both online and offline, however, its sufficiency and alignment with international principles can be discussed separately.

Chapter 9 of the Privacy Act provides for privacy of electronic means. According to Section 19, every individual has the right to maintain the privacy of their personal information, documents, correspondence, data, and character stored electronically, and unauthorized access, violation, or disclosure of such information is prohibited. Similarly, the law prohibits listening to or recording conversations between individuals using electronic means without consent or legal authorization.

[41] Article 22

[42] Article 28

[43] Preamble, The Privacy Act, 2075

Other Legal Provisions

The Copyright Act, 2059 (2002) protects the copyright of ideas, including a computer program. It prohibits people from copying and modifying the original work of others, and using it for their own advantage or economic benefits.

Electronic Transactions Act, 2063 (2006), can be regarded as the first cyber law in Nepal. This Act legalized the transaction of electronic records in Nepal. It includes the provision relating to electronic records and digital signature, provision relating to the computer network and network services providers, provision relating to dispatch, receipt and acknowledgement of electronic records. Section 48 of the Act prescribes the persons having access to data not to divulge or causes to divulge confidentiality of any record, books, registers, correspondence, information, documents or materials to any unauthorized person. However, there is no explicit provisions dealing with privacy and data protection.

Nepal Telecommunications Authority (NTA) has framed ***Cyber Security Byelaw, 2077 (2020)*** by exercising the rights conferred under Section 62 of the Telecommunications Act, 2053 (1997) for the implementation of cyber security standards and best practices. This bylaw has provided a checklist for Information System (IS) audit. It is a mandatory cybersecurity regulation for Telecommunication Service Providers (TSPs) and Internet Service Providers (ISPs) to systematically implement security standards and best practices. Moreover, the regulations make it mandatory for service providers (TSPs and ISPs) to perform a security audit.

Besides above, Nepal Rastra Bank has been enforcing ***Information Technology Guidelines 2069 (2012)*** in banking and financial sectors which set standards for information technology and information security required to be followed by financial sectors.

D. Emerging Challenges in Privacy and Data Protection

Privacy and data protection are equally important online and offline. However, the rapid digitalization and development of Cloud Computing, Autonomous Vehicles, Artificial Intelligence, Big Data, and Machine Learning have enormous potential[44] as well as challenges for data security and privacy. Artificial Intelligence (AI) and its applications are a part of everyday life nowadays, from social media news feeds to mediating traffic flow in cities to autonomous cars to connected consumer devices such as smart assistants, spam filters, voice recognition systems, and search engines.

Some major data privacy risk areas related to new technologies can be outlined as follows:

- New technologies such as AI can be used to identify and track individuals across different devices in their homes, at work, and in public spaces. For example, through the application of facial recognition technology, based on AI, individuals can be tracked and identified.
- AI-driven identification, profiling and automated decision-making can lead to discriminatory or biased outcomes. People can be misclassified, misidentified, or judged negatively, and such errors or biases may disproportionately affect certain demographics.
- People are often unable to fully understand what kinds of and how much data their devices, networks, and platforms generate, process, or share. As consumers continue to introduce smart and connected devices into

[44] Dhirani, L.L.; Mukhtiar, N.; Chowdhry, B.S.; Newe, T. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors 2023, 23, 1151. https://doi.org/10.3390/s23031151

their homes, workplaces, public spaces, and even bodies, the need to enforce limits on data exploitation has become increasingly pressing.

- AI can utilize sophisticated machine-learning algorithms to infer or predict sensitive information from non-sensitive forms of data. For instance, someone's keyboard typing patterns can be analyzed to assume their emotional state, which includes emotions such as nervousness, confidence, sadness, or anxiety. Even more alarming, a person's political views, ethnic identity, sexual orientation, and even overall health status can also be determined based on activity logs, location data, and similar metrics.

  To regulate and avoid the potential risk, a comprehensive privacy and protection law and enforcement infrastructure is required in place. Further, the user also should be aware and be able to have a minimum impact assessment.

Chapter 5
Information Integrity

Information integrity ensures that data maintains its accuracy and reliability from creation to disposal, retaining its intended meaning without unauthorized changes or corruption. Safeguarding the trustworthiness of information requires implementing diverse measures, including encryption, access controls, and routine quality assessments, to prevent compromise.

A. Importance of Information Integrity in the Digital Era

In the digital era, maintaining information integrity is essential for safeguarding data, fostering trust, and preserving the credibility of digital infrastructures. It ensures reliability, protects against cybersecurity threats, and upholds regulatory compliance. In Nepal, with the emerging digital landscape, prioritizing information integrity is paramount for sustainable progress and development. Here's why it's imperative:

1. **Legal compliance**: In Nepal, regulations such as the Privacy Act of 2075 (2018) mandate that organizations safeguard personal data. Failure to adhere to these regulations may result in legal repercussions and damage an organization's reputation.
2. **Trust and credibility:** Trust and credibility in digital systems, such as those employed by Nepal's government, hinge on the reliability of information. For example, census data informs strategic planning and policy-making. If data integrity is compromised, it could result in flawed decisions and undermine public trust in the government's resource management capabilities.

3. **Security and privacy protection:** Information integrity is crucial for security and privacy, especially in Nepal's growing digital payment systems. Protecting financial transactions keeps sensitive data safe and prevents fraud. Without integrity measures, data breaches could lead to financial losses.

4. **Data reliability:** Data integrity is crucial for decision-making, like in Nepal's healthcare system where electronic health records (EHRs) are used. Keeping these records accurate is vital for correct diagnoses and safe treatment. Manipulating or accessing them without authorization could lead to serious medical mistakes.

B. Disinformation, Misinformation, and Fake News

Disinformation is the intention to spread false news meant to deceive. Misinformation, on the other hand, is false information shared mistakenly. Fake news refers to fabricated stories aimed at tricking people. These types of misinformation make it challenging to make informed decisions and discuss important topics. That's why it's crucial to cultivate critical thinking skills and verify facts.

- **Disinformation:** Disinformation refers to intentionally false or misleading information spread to deceive or manipulate people's opinions. It is often created by individuals, groups, or even governments with particular objectives in mind. Disinformation can be encountered on various platforms such as social media, news outlets, and everyday conversations. Its primary goal is to sow confusion, undermine trust, or promote specific agendas, regardless of their accuracy. For example, in Nepal, a political party might fabricate fake social media profiles to disseminate false information about a competitor, aiming to influence voters and tarnish their reputation.

- **Misinformation:** Misinformation refers to incorrect information shared unintentionally, without the intent to deceive. It often stems from errors, misunderstandings, or outdated facts. Misinformation spreads rapidly across online platforms and in conversations, leading to confusion and negative consequences. For example, during a health crisis in Nepal, individuals might unknowingly share false information on social media regarding traditional remedies, believing in their effectiveness. While they may not have harmful intentions, this misinformation can create false hope, delay proper treatment, and exacerbate the crisis.
- **Fake news:** Fake news consists of fabricated stories crafted to deceive people. Despite appearing genuine, fake news stories lack truthfulness. They are often created to attract clicks, promote specific agendas, or cast doubt on legitimate news sources. Fake news proliferates rapidly on social media platforms and has the potential to influence people's opinions. To combat fake news, it's crucial to verify facts and employ critical thinking skills. For example, a website might publish a fake news article claiming that a well-known temple in Nepal is haunted. Although untrue, such misinformation could instill fear and damage the temple's reputation.

C. Strategies for Promoting Information Integrity Online

To enhance information integrity online, various strategies are employed to cultivate trust, accuracy, critical thinking, and transparency. Nepal can effectively bolster information integrity online by adopting several key approaches:

- **Transparency and accountability:** Encouraging content creators and online platforms to be transparent about their policies and affiliations fosters trust and accountability.

- **Digital literacy:** Educating individuals in critical thinking and digital skills empowers them to discern reliable information and make informed choices online.
- **Promotion of reliable sources:** Encouraging reliance on credible sources aids individuals in accessing accurate information while avoiding unreliable sources.
- **Fact-checking initiatives:** Establishing fact-checking groups or initiatives to verify online content helps curb the dissemination of false information.
- **Collaboration and partnerships:** Collaborating with government bodies, civil society organizations, and tech companies on initiatives to promote information integrity leverages collective knowledge and resources, leading to more effective outcomes.

Chapter 6
Internet Governance

A. Evolution and History of Internet Governance

Internet governance refers to the processes and mechanisms that shape how the internet is managed and controlled. As a global resource, internet is not managed or controlled by a single country, a single agency or a single company. It involves a wide range of stakeholders, including governments, private companies, civil society organizations, and technical experts, who work together to ensure the smooth functioning of the internet and address various challenges and issues related to its use.

There are many agencies involved in the internet governance. Internet-specific organizations emerged in the 1980s to address coordination needs, primarily led by technologists. The International Telecommunication Union (ITU) played a pivotal role in global telecommunications governance, particularly with the adoption of the International Telecommunication Regulations (ITRs) in 1988, facilitating liberalization and interoperability.

Technical bodies such as the Internet Architecture Board, Internet Engineering Task Force (IETF), and Internet Society (ISOC) emerged to coordinate Internet protocols and standards development. The IETF, in particular, operates as a consensus-based organization involving various stakeholders. ISOC provided institutional support to these bodies, fostering collaboration and standardization.

The Internet Assigned Numbers Authority (IANA) managed the allocation of unique names and numbers in the global network. In 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was established to oversee IANA functions, marking a transition to a more formal governance structure.

ICANN's creation led to debates over internet governance, particularly concerning the role of governments and multi-stakeholderism. The Governmental Advisory Committee (GAC) was established within ICANN to provide government input, reflecting the growing political nexus in internet governance.

The UN Information and Communication Technologies Task Force (UNICT) provided a platform for dialogue on internet governance, advocating for multi-stakeholder involvement. However, multi-stakeholder groups also raised concerns about dominance and legitimacy, particularly among developing countries.

Overall, internet governance evolved from informal coordination among technologists to a more structured multi-stakeholder approach, reflecting the complex and interconnected nature of the Internet ecosystem.

B. Multi-Stakeholder Approach to Internet Governance

The Multi-stakeholder Model was recognized at the World Summit on the Information Society (WSIS) as the global model for Internet governance; WSIS outcome documents (2005) provided a set of framework principles for the multistakeholder model.

“A working definition” of Internet governance was developed by the Working Group on Internet Governance (WGIG) and later adopted by the Summit and included in para. 34 of the Tunis Agenda, which states that Internet Governance is “the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet".

The roles and responsibilities of each stakeholder group are further specified in para. 35 of the Tunis Agenda, which states that: "The management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect, it is recognized that:

1. Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.
2. The private sector has had and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.
3. Civil society has also played an important role in Internet matters, especially at the community level, and should continue to play such a role.
4. Intergovernmental organizations have had and should continue to have, a facilitating role in the coordination of Internet-related public policy issues.
5. International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies".

Based on the multistakeholder model adopted at the WSIS, most of the organizations engaged in the internet governance recognize and use multistakeholder model. For example, the ITU multistakeholder membership includes governments, regulators, industry, international organizations (intergovernmental and non-governmental), financial institutions, and civil society. ITU’s membership ranges from mobile and fixed phone operators to satellite companies, from equipment vendors to broadcasters and Internet Service Providers (ISPs). It also includes organizations focusing on access for people with disabilities, for example, or on emergency communications. ITU members also include various Internet-related organizations and academic institutions, including universities and research institutes focusing on ICTs.

C. Role of Governments, Civil Society, and Private Sector in Internet Governance

The governance of the Internet is a multifaceted and collaborative endeavor that involves a diverse range of stakeholders, each playing a vital role in shaping policies and practices. The World Summit on the Information Society (WSIS) has provided a comprehensive framework for understanding these roles, emphasizing the importance of cooperation among governments, the private sector, civil society, and other organizations.

Governments hold a crucial responsibility in the realm of Internet governance. Their roles and responsibilities include public policymaking and coordination at national, regional, and international levels. This involves creating an enabling environment for ICT development, overseeing the implementation of ICT policies, and developing and enforcing laws, regulations, and standards. Governments also foster international cooperation, promote capacity-building initiatives, ensure cybersecurity, and encourage the development of ICT infrastructure and applications. Additionally, they play a significant role in promoting cultural diversity, facilitating dispute resolution, and addressing general developmental issues within the digital realm.

The private sector is instrumental in driving the development and implementation of Internet technologies and practices. Their roles and responsibilities include industry self-regulation, contributing to policy proposals, and developing best practices and tools for policymakers and stakeholders. The private sector is heavily involved in research and development, fostering innovation, and participating in national and international policy development. They also engage in arbitration and dispute resolution, promote capacity-building initiatives, and help shape the future of Internet technologies and standards through their extensive R&D efforts.

Civil society organizations (CSOs) play a vital role in ensuring that Internet governance remains inclusive and reflective of public interests. Their roles and responsibilities include raising awareness about digital rights, fostering capacity-building through knowledge sharing and training, and advocating for public interest objectives such as human rights, social justice, and sustainable development. CSOs facilitate network-building among stakeholders, mobilize citizens for democratic processes related to Internet governance, and bring marginalized perspectives into policy discussions. They are active in policy engagement, ensuring processes are bottom-up and people-centered, and they encourage social responsibility and good governance practices within the digital realm. Additionally, CSOs contribute to the R&D of technologies and standards that serve the public good and hold political and market forces accountable to societal needs.

The academic and technical communities are key contributors to the development and stability of the Internet. They provide innovative solutions and ideas that drive the evolution of the Internet, set technical standards, and ensure the stable operation of Internet services. These communities collaborate extensively with all stakeholder groups, sharing expertise and contributing to policy development.

The WSIS has highlighted the need for improved coordination among intergovernmental and international organizations involved in Internet governance. By fostering formal and informal consultations, these organizations can better align their efforts and address the complex challenges of managing the global Internet.

Effective Internet governance relies on the collaborative efforts of governments, the private sector, civil society, and the academic and technical communities. Each stakeholder brings unique perspectives and capabilities, making their contributions essential for creating a balanced, inclusive, and forward-looking digital environment. As the Internet continues to evolve, ongoing cooperation and dialogue will be key to addressing new challenges and opportunities in the digital age.

Chapter 7

Digital Safety Measures

A. Threat Landscape in the Digital Environment

In today's digital world, the Internet is a big part of our daily lives for people of all ages and backgrounds. While it offers many benefits, it also comes with risks and threats that we need to be aware of. As we explore new technologies, staying safe is very important.

The internet's pervasive growth over the past decade has been staggering, encompassing approximately 67% of the global population and connecting 5.4 billion individuals worldwide, alongside over 15 billion IoT devices. However, this expansion has also broadened the scope of threat vectors, with every connected device presenting a potential target from the perspective of threat actors.

Various threats plague the digital landscape, including misinformation, disinformation, hate speech, cyberbullying, sexual exploitation, and identity theft. These threats can be categorized into access denial, unauthorized access, exposure of private and sensitive data without permission, and other personal attacks such as hate speech, cyberbullying, harassment, and abuse, as well as misinformation and disinformation.

The following sections cover some of the most common digital threats:

Malware

Malware, or “malicious software,” is an umbrella term that describes any malicious program or code that is harmful to systems[45]. Malware is hostile, intrusive, and intentionally harmful software designed to invade, damage, or disable computers, systems, networks, tablets, and mobile devices, often taking partial control of a device’s operations. Similar to the human flu, it disrupts normal functioning.

Malware has different purposes. It can be used to make money from victims, disrupt work, make political statements, or show off skills. While malware usually can't damage the physical hardware of computers or network equipment, it can steal, encrypt, or delete data, change important computer functions, and spy on computer activity without the user knowing or giving permission.

Ransomware

Ransomware is a type of malware that prevents you from accessing your device and the data stored on it, typically by encrypting your files. A criminal group will then demand a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen, or deleted. Attackers may also threaten to leak the stolen data.

Ransomware operates by first gaining access to your network, where attackers establish control and deploy malicious encryption software. Once activated, the malware locks devices and encrypts data, rendering it inaccessible.

D-DOS Attack

A Distributed Denial-of-Service (DDoS) attack is a cybercrime where the attacker overwhelms a server with internet traffic to prevent users from accessing online services and sites. Botnets are the primary means by which DDoS attacks are executed. Attackers hack into computers or other devices and install malicious software, or malware,

[45] https://www.malwarebytes.com/malware

called bots. These infected devices collectively form a network, or botnet, used to carry out the attack. In January 2024, Nepal government's main server had faced D-DOS cyberattacks leading to disruptions of hundreds of government websites across the country[46].

Phishing

"Phishing" refers to a deceptive practice aimed at obtaining sensitive information, such as usernames, passwords, credit card numbers, or bank account details, typically for illicit use or resale. It involves impersonating a trusted entity, often through email or text messages, to lure unsuspecting victims into divulging their personal data. Similar to a fisherman using bait to catch fish, the attacker crafts convincing communications to entice the victim. Phishing is a major threat where attackers try to steal money, get confidential information, or install malware on the victim's device. This harmful tactic is becoming more common in cyberattacks.

Cyber Bullying

Cyberbullying is when someone uses the internet or electronic devices to harass, threaten, or humiliate others. It can happen through social media, text messages, emails, or online games. Cyberbullying can make people feel scared, sad, or embarrassed, and it can be very hurtful. It's important to speak up and get help if you or someone you know is being bullied online. The cases of cyber-bullying have been constantly increasing in Nepal and as per Nepal Police data, cyber-bullying through social media is most common.

Hate Speech

Hate speech is any communication that belittles or discriminates against people based on their race, religion,

[46] https://kathmandupost.com/national/2024/01/01/government-s-main-server-faces-cyberattacks

gender, sexual orientation, or other characteristics. In theory, it involves using harmful language to spread hatred and incite violence against specific groups. In practice, hate speech can be found in social media posts, comments, messages, and even videos. It poses a significant threat in the digital space, as it can lead to real-world harm, discrimination, and division among communities. It's crucial to recognize and address hate speech to create a safer and more inclusive online environment.

Misinformation/Disinformation

Misinformation/disinformation are false or misleading information. Misinformation is when incorrect information is shared without intending to cause harm, while disinformation is deliberately created to deceive people. Mis/disinformation spread much faster online, compared to offline. Mis/disinformation can be found in fake news articles, social media posts, and manipulated videos. Recently in Nepal, an online news portal called 'Sidha Kura' had published a series of news regarding involvement of media publishers and Supreme Court judges in manipulating court verdict[47]. However, the forensic investigation revealed that the sting operation video tape was fake and the news actually was disinformation[48]. The case is still ongoing in the Supreme Court. The threats of mis/disinformation in the digital space can lead to misunderstandings, mistrust, and even dangerous actions. It's important to check the accuracy of what we read and share online to help combat these issues.

B. Best Practices for Digital Safety

Staying safe online is crucial because our personal and sensitive information is often shared and stored on the internet. Cyber threats like hacking, phishing, and malware

[47] https://myrepublica.nagariknetwork.com/news/sc-directs-sidhakura-news-portal-to-appear-with-evidences-on-may-2/

[48] https://en.setopati.com/social/163194

can steal our data, invade our privacy, and cause financial and emotional harm. Additionally, our online activities can make us targets for cyberbullying, scams, and identity theft. By understanding the importance of online safety, we can take steps to protect ourselves and our loved ones from these dangers, ensuring a more secure and enjoyable digital experience.

Here are some best practices for staying safe online:

Create Strong Passwords:

Using strong passwords is essential for protecting your online accounts. A strong password includes a mix of uppercase and lowercase letters, numbers, and special characters, making it harder for others to guess or crack. Aim for at least eight characters to enhance security. For example, "P@ssw0rd!23" is much more secure than "password123."

Combine Random Words:

A passphrase made of random words is more secure than a simple password. Choose three unrelated words and combine them to create a unique passphrase. Add numbers and special characters to further increase its strength. For example, "DogBananaSky!2024" is both memorable and secure.

Avoid Reusing Passwords:

Using the same password for multiple accounts increases the risk of all your accounts being compromised if one is hacked. Create a unique password for each account to ensure that if one password is breached, your other accounts remain secure. This practice significantly enhances your overall online security.

Use a Password Manager:

Remembering multiple complex passwords can be challenging. Password managers securely store and manage your passwords, allowing you to use strong, unique passwords for each account without needing to remember them all. You only need to remember one master password, and the password manager handles the rest.

Avoid Simple Passwords:

Simple passwords, like names or common phrases, are easy to guess and therefore insecure. Many apps and websites now require more complex passwords, but common ones like '1Qwerty!' are still unsafe. Always create passwords that are hard to predict to keep your accounts protected.

Enable Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA)

To enhance your online security, enable Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA). These methods add an extra layer of protection beyond just passwords, making it harder for cybercriminals to access your accounts. Make sure to turn on 2FA for your most important accounts, such as email, banking, social media, and online shopping. Even if your password is stolen or compromised through a data breach, 2FA can help prevent unauthorized access to your accounts by requiring an additional verification step. This simple action significantly improves your online safety.

Keep Your Software and Operating System Updated

Keep your devices safe by regularly updating their software. This includes the operating systems on your phones, tablets, and laptops, as well as all your apps and web browsers. Software updates often contain security patches that fix vulnerabilities and protect you from online threats. Enable automatic updates to ensure your devices stay secure without manual intervention. Applying these updates promptly is one of the simplest and most effective ways to enhance your digital safety.

Avoid Online Scams and Phishing Attacks

Be careful with emails from unknown senders. Avoid clicking on links or downloading attachments from suspicious emails. Check sender email addresses for legitimacy and watch for signs of phishing, like spelling errors or urgent requests for personal information. Download files only from trusted sources to prevent malware attacks.

When browsing websites, be cautious of links or pages that seem too good to be true. Avoid clicking on unfamiliar links or engaging with questionable online content. If you receive an email that raises doubts, do not click on links or open attachments. Instead, verify the email's legitimacy directly with the sender, such as your bank, to avoid falling for phishing scams. Trust your instincts and stay cautious to protect yourself from online threats.

Keep Your Devices Safe

To protect your computers, laptops, smartphones, and tablets, start by installing reliable antivirus software. Regular scans help identify and remove threats. For added security, use anti-malware tools to defend against viruses, malware, and digital intrusions. Stay alert by keeping your operating system and applications up to date. Updates are crucial for enhancing security and protecting your devices and data from potential threats. Choose a reputable antivirus provider and keep your internet security software current. This helps defend against common and advanced threats like viruses, spy apps, "cryptolockers," and XSS attacks. Regular updates ensure your antivirus software can combat the latest cyber threats effectively.

Additionally, use built-in security features like Windows Defender for genuine Windows users. Mac OS and Linux also offer inherent security measures that provide extra layers of protection against malware and cyber threats."

Protect Your Online Presence

Always remember that once you post something online, it can be difficult to delete it completely. Avoid sharing personal details such as your social security number, address, or date of birth on social media platforms. It's wise to be cautious with your email address; consider using a secondary account for sign-ups and subscriptions to safeguard your primary one. When making online purchases, only provide sensitive information on secure, encrypted websites.

It's crucial for both children and family members to understand the importance of managing their online presence. They should be aware of what is appropriate to share on the internet and what should be kept private. Remember that anything posted online, whether a comment or image, can potentially remain there indefinitely. Even if you delete the original post, copies made by others may still exist.

Protect Your Data

Ensuring the safety of your personal data is crucial in today's digital world. One important step is to regularly back up your important files to an external hard drive or cloud storage. This helps protect your data from threats like ransomware, which can lock your computer and prevent access to your files. Additionally, using security software can further protect your data from malware.

Backing up your data is simple but essential. It involves making copies of your important files and storing them in a safe place, such as cloud storage or a USB drive. This way, if you lose your device or it gets damaged, you can still access your data. Using cloud storage offers the convenience of automatic backups and accessibility from anywhere, but it's important to use strong passwords and enable features like two-factor authentication to keep your backups secure.

C. Digital Rights Vis-a-Vis Digital Safety

In today's digital age, digital rights and digital safety are intricately connected, shaping how we interact and navigate the online world. Digital rights encompass the freedoms and protections that individuals are entitled to online, ensuring that everyone can use the internet freely and securely. These rights include the right to privacy, which is crucial for safeguarding personal information from unauthorized access and ensuring a sense of security in our digital interactions. Additionally, digital rights include the freedom of expression, allowing individuals to voice their opinions and ideas without fear of censorship or reprisal. This freedom is fundamental for fostering open dialogue and diverse perspectives in the digital sphere.

The right to privacy is a fundamental aspect of digital rights, highlighting the importance of protecting personal information online. With the increasing prevalence of data collection and sharing practices, understanding how your data is used and taking proactive measures to protect it are essential. By being aware of privacy policies, using secure passwords, and being cautious about sharing personal information, individuals can protect their privacy and minimize the risk of identity theft or other online threats.

Moreover, digital safety is closely tied to the freedom of expression. While individuals have the right to express themselves online, it is important to do so responsibly, considering the impact of their words and actions on others. Creating a safe and respectful online environment involves respecting the rights and opinions of others, avoiding harmful or offensive content, and promoting positive interactions. By upholding these principles, individuals can contribute to a more inclusive and secure digital world where everyone can freely express themselves while respecting the rights of others.

Chapter 8

AI and Digital Rights

A. Background

Artificial Intelligence (AI), refers to computer systems that can perform tasks that typically require human intelligence, such as learning, reasoning, and problem-solving. AI technologies include machine learning, which allows computers to learn from data and improve over time, and natural language processing, which enables computers to understand and generate human language.

In Nepal, various AI tools are gaining traction, including virtual assistants, image recognition systems, and predictive analytics. AI continues to advance, with increasing applications expected across diverse sectors, enhancing functionality and enriching lives. Here are some examples relevant to Nepal, along with their respective use cases:

1. **Chatbots**: In Nepal, businesses use chatbots for customer support. Chatbots can answer questions, give product info, and guide users on websites or apps, making it easier for customers to get help.
2. **Image recognition**: In Nepali agriculture, image recognition helps with tasks like crop monitoring. Drones take pictures of farmland, and AI analyzes them to spot crop problems or areas needing care, like pest infestations or low yields.
3. **Recommendation systems**: Nepali e-commerce sites use recommendation systems to suggest products. These systems look at what users like and recommend similar items, making shopping easier and boosting sales.

4. **Predictive analytics**: In Nepali healthcare, predictive analytics helps analyze patient data to predict outcomes. For instance, it can identify high-risk patients for diseases like diabetes or heart disease, so doctors can intervene early with personalized treatment plans.

5. **Traffic management**: In Nepal, the Traffic Police use AI to manage traffic. They use cameras, sensors, and GPS to analyze traffic, spot violations, and predict jams to make roads safer.

6. **Speech recognition**: In Nepali schools, speech recognition tools help students learn and access content. These tools turn spoken Nepali into text, making it easier for students with hearing impairments or language difficulties to participate in class and learn.

Digital Rights: Digital rights refer to the freedoms and protections individuals have online. They include the right to privacy, the right to freedom of expression, and other relating rights. These rights ensure that people can use the internet and digital technologies safely, freely, and fairly. In Nepal, these rights are increasingly significant as more aspects of our lives transition to the digital realm. They encompass the ability to express oneself freely online, safeguard personal information, and access unrestricted information. Here are some examples relevant to Nepal, along with their corresponding use cases:

1. **Freedom of Expression**: Nepali citizens can express themselves freely online, including on social media. They can use the internet to support causes like human rights and environmental protection. They can criticize the government or draw their attention to corruption or mismanagement through online expression.

2. **Access to Information**: Nepali citizens can access government information and public data online.

Programs like open government data in Nepal make government information available online, so people can learn about services, budgets, policies, and projects.

3. **Right to privacy**: Nepali citizens have the right to keep their digital communications and personal data private. Laws like the Individual Privacy Act, 2018 helps protect people's privacy by regulating the processing and management of personal information.

4. **Online harassment and cyberbullying**: Nepali citizens should be safe from online harassment and cyberbullying. Proposed draft on Social Media Regulation or Information Technology and Cybersecurity, aim to address the cybercrimes like harassment, bullying, and identity theft, protecting people's rights and safety online.

B. Implications of Artificial Intelligence on Digital Rights

The impact of AI on digital rights is multifaceted, encompassing both positive and negative outcomes. Addressing this necessitates a balanced approach that maximizes AI benefits while safeguarding digital rights. This entails robust regulations, ethical considerations, and mechanisms for accountability to protect fundamental rights in the digital age.

Several key implications include:

1. **Algorithmic bias and discrimination**: AI algorithms may inadvertently perpetuate biases present in the data they learn from, leading to unfair treatment, particularly for marginalized groups. This can undermine digital rights such as equality and equitable access to opportunities.

2. **Data protection**: AI's utilization in data processing can pose challenges in adhering to data protection

regulations like GDPR. This increases the risk of data breaches and potential discrimination by algorithms, impinging on individuals' rights to safeguard their personal data.

3. **Privacy concerns**: AI systems rely heavily on data, including personal information, raising privacy concerns regarding data collection, analysis, and sharing without individuals' consent or adequate safeguards.

4. **Digital divide**: AI adoption may exacerbate the digital divide by widening disparities between those with access to technology and those without. This can hinder individuals' participation in the digital sphere, access to education, and engagement in society, exacerbating existing inequalities.

C. Ethical Considerations in AI Development and Deployment

Ethical considerations play a pivotal role in the development and deployment of AI. Prioritizing ethics ensures that AI is responsible, accountable, and aligned with the needs of individuals.

Key ethical considerations include:

1. **Accountability and governance**: Establishing clear rules and oversight mechanisms is essential to ensure responsible AI usage. Developers, organizations, and policymakers should delineate roles and procedures for addressing ethical concerns and complaints related to AI.

2. **Privacy and data protection**: AI systems must uphold individuals' privacy rights and comply with data protection regulations. Developers should employ techniques like data encryption and obtain consent before collecting or utilizing personal data.

3. **Bias mitigation**: It's imperative to train AI models to mitigate biases and ensure fairness for all individuals.

Developers should use diverse datasets and actively monitor for bias during the development process, taking measures to ensure AI decisions are impartial and unbiased.

4. **Human-centered design**: AI should be designed with human well-being and dignity in mind. Developers should involve diverse stakeholders in the design process, prioritizing safety, accessibility, and inclusivity for users.

5. **Ethical review and improvement**: Ethics should be integrated into every stage of AI development. Developers should continually review and enhance ethical standards throughout the AI lifecycle, fostering responsible innovation and ethical conduct within the AI community.

6. **Transparency and accountability**: Building trust in AI systems requires transparency regarding their functioning. Developers should provide explanations of algorithms, data sources, and decision-making processes, enabling users to understand and trust AI systems.

D. Regulatory Frameworks for AI and Digital Rights Protection

Regulatory frameworks for AI and digital rights differ globally, adapting to technological advancements. While Nepal's regulations are in the early stages, there's an opportunity to align with international standards, engage stakeholders, and establish robust frameworks for responsible AI deployment and safeguarding digital rights. Collaboration among government, industry, civil society, and academia is crucial for shaping Nepal's approach to AI governance and digital rights protection.

An overview of regulatory frameworks, both globally and in Nepal:

Globally	Nepal
General Data Protection Regulation (GDPR) The General Data Protection Regulation (GDPR), enforced by the European Union (EU), stands as a prominent global data protection regulation. It establishes stringent guidelines governing the collection, processing, and storage of personal data, with an emphasis on transparency, consent, and the protection of individuals' rights. The GDPR applies to any organization handling the personal data of EU residents, irrespective of their geographical location.	**Data Protection and Privacy Laws** Nepal has enacted the Privacy Act, of 2075 (2018), which regulates the collection and processing of personal data. Additionally, the Electronic Transactions Act of 2008, along with its associated regulations, provides guidelines for electronic transactions, encompassing provisions for data protection and privacy.

Globally	Nepal
AI Policy and Regulatory Initiatives in the United States The United States currently lacks comprehensive federal regulation dedicated solely to AI, several federal agencies have initiated policy dialogues and guided on AI-related matters. Furthermore, certain states have enacted their legislation or executive orders pertaining to AI governance, privacy, and ethics.	**Cybersecurity and Information Technology Laws** Nepal has laws and regulations pertaining to cybersecurity and information technology, which may indirectly impact aspects of AI governance and digital rights protection. For instance, the Cyber Security Policy 2023 aims to enhance cybersecurity measures to protect critical information infrastructure and combat cyber threats
OECD Principles on AI The OECD has developed principles on AI to promote the responsible governance of AI technologies. These principles prioritize human values, transparency, accountability, and inclusivity, guiding governments, industry, and civil society in shaping AI policies and practices.	**Emerging Policy Initiatives** Nepal is exploring policy initiatives for emerging technologies such as AI. There is potential to incorporate AI governance, digital rights protection, and ethical considerations into broader frameworks for technology, innovation, and digital transformation.

Chapter 9

Digital Literacy/Inclusion

Digital literacy and inclusion are essential for enabling full participation in the digital realm. Digital literacy entails effectively using and understanding digital technology, as well as discerning online information. It encompasses skills such as computer usage, internet comprehension, and awareness of cybersecurity. Digital literacy facilitates information access, communication, and problem-solving online.

Digital inclusion aims to ensure universal access to digital technology and opportunities, regardless of background. It involves overcoming barriers related to access, affordability, and skills, particularly for underserved groups. Digital inclusion efforts mitigate inequalities and enable broad participation in the digital economy and society.

By prioritizing digital literacy and inclusion, society can optimize digital technology, foster inclusivity, and support sustainable development.

A. Importance of Digital Literacy in Promoting Digital Rights

Digital literacy plays a crucial role in supporting digital rights by fostering awareness, encouraging critical thinking, enhancing security and privacy, accessing information and services, and empowering advocacy for digital rights.

Some of the significant roles include:

1. **Access to information and services**: Digital literacy equips individuals with the skills to effectively utilize digital tools and services, granting them access to

information, education, government services, job opportunities, and community engagement. By eliminating barriers to digital access, literacy promotes equal opportunities and inclusion, thereby supporting digital rights for all.

2. **Digital security and privacy**: Digital literacy empowers individuals to understand and mitigate cybersecurity and privacy risks, enabling them to safeguard their personal information and identities. Through knowledge of techniques like encryption and secure passwords, individuals can uphold their digital rights to privacy and security.

3. **Awareness of digital rights**: Digital literacy educates individuals about their rights and responsibilities online, including privacy, freedom of speech, and protection from harassment. By being informed about their rights, individuals can advocate for themselves, speak out against violations, and demand respect for their digital rights from both companies and governments.

4. **Critical thinking and literacy**: Digital literacy fosters critical thinking skills in assessing online information. By discerning reliable sources from unreliable ones, individuals can navigate the online landscape safely, protect their digital rights, and make informed decisions online.

B. Strategies for Promoting Digital Inclusion

Promoting digital inclusion involves addressing barriers to access, affordability, connectivity, and skills, ensuring universal participation in the digital realm. Through coordinated efforts, stakeholders can bridge the digital divide and ensure equitable access to the benefits of the digital age.

Here are some strategies:

1. **Internet connectivity**: Enhance internet accessibility in rural areas by expanding affordable and reliable broadband connections. Collaborate with communities, businesses, and governments to implement projects that extend broadband coverage to underserved regions and narrow the digital gap.
2. **Policy and advocacy**: Advocate for policies that foster digital inclusion, such as initiatives to improve internet infrastructure and allocate funding for digital literacy programs. Collaborate with governmental bodies, businesses, and nonprofit organizations to develop comprehensive strategies for inclusion at various levels.
3. **Digital literacy education**: Integrate digital skills training into school curricula, vocational programs, and adult education initiatives. Emphasize critical thinking, online safety, and responsible internet usage to equip individuals with the necessary skills for full participation in the digital world.
4. **Affordable access to technology**: Make digital devices, such as computers, tablets, and smartphones, accessible to underserved populations through subsidies, discounts, or loan programs. Ensure that low-income families have affordable access to technology to facilitate their inclusion in the digital ecosystem.
5. **Public awareness and outreach**: Raise awareness about the importance of digital inclusion through public campaigns, events, and outreach activities. Promote digital literacy, disseminate information about available resources, and encourage participation in inclusion programs to foster a digitally inclusive society.

C. Addressing Barriers to Digital Literacy and Inclusion

To address barriers to digital literacy and inclusion comprehensively, a multifaceted approach is necessary, targeting factors contributing to disparities in access, skills, and engagement in the digital domain.

Here are some strategies for overcoming these barriers:

1. **Affordable access to technology**: Make digital devices, such as computers, tablets, and smartphones, more accessible to low-income families by implementing discount programs and offering refurbished device initiatives. Collaborate with tech companies, nonprofits, and communities to distribute discounted or donated devices to underserved groups.
2. **Infrastructure development**: Enhance internet accessibility in rural areas by expanding broadband and wireless technology infrastructure. Encourage private sector investment through subsidies and incentives to connect marginalized communities and improve overall internet access.
3. **Policy advocacy and collaboration**: Advocate for supportive policies and funding for digital literacy and inclusion initiatives, including training programs and enhanced internet access. Forge partnerships with governments, nonprofits, businesses, and communities to pool resources and collectively address barriers to digital inclusion.
4. **Digital skills training programs**: Provide affordable digital skills training programs tailored to diverse groups, covering fundamental topics such as computer use, internet safety, and job readiness. Partner with educational institutions, libraries, community centers, and employment agencies to deliver accessible training opportunities for individuals of all ages and backgrounds.
5. **Community-based initiatives**: Establish community learning centers or digital hubs where individuals can

access technology training, attend workshops, and participate in educational programs. Empower local leaders, educators, and volunteers to facilitate digital literacy classes, mentorship programs, and peer learning activities.

6. **Tailored support**: Offer specialized assistance and resources to groups facing specific challenges in digital literacy and inclusion, such as seniors, individuals with disabilities, immigrants, refugees, and those with low literacy levels. Develop customized training materials, assistive technologies, and support services to address their unique needs effectively.

Chapter 10
E-Governance / Services

A. Background

To understand e-governance, firstly we need to understand 'governance' which is difficult to define in a single sentence. Broadly, governance is related to a system and process of state functioning and service delivery to the public.

The concept of 'governance' derived along with the concept of the 'government'. Governance is also an idea and notion to connect and interact with people. That is why questions will arise about how, what, and for whom the government and governance are required. The government and the governance are for solving the people's concerns democratically using state authority.

Rule of law, transparency, accountable and efficient government, adherence to the human rights concept, and democratic exercise of power are the fundamental dimensions of governance.

As stated above, it is difficult to define, but to cover its dimension and understand easily, the definition proposed by the International Institute of Administrative Science (IIAS) has covered the wider meaning of governance,[49] which includes:

- "Governance refers to the process whereby elements in society wield power and authority, and influence and enact policies and decisions concerning public life, and economic and social development."

[49] extracted from the Article written by Frank Bannister and Regina Connoiiy, Defining E-Governance, e-Service Journal · January 2012

- "Governance is a broader notion than government, whose principal elements include constitution, legislature, executive and judiciary. Governance involves interaction between these formal institutions and those of civil society."
- "Governance has no automatic normative connotation. However, typical criteria for assessing governance in a particular context might include the degree of legitimacy, representativeness, popular accountability, and efficiency with which public affairs are conducted.

E-governance is the elaboration of the same notion of the transformation of the governance paradigm in the digital world. With the development of the information and communication technology (ICT), the process of delivery of government services has been shifted and technology has become a dominant factor. Electronic governance or e-Governance is the idea of the application of ICT in the delivery of government services through the integration of various systems between Government-to-Citizens (G2C), Government-to-Business (G2B), and Government-to-Government (G2G).

E-governance is also called digital governance, internet governance, etc. E-gov is another facet of good governance and it equally requires the application of basic dimensions of good governance, those which are- the rule of law, transparency, efficiency, and accountability in the process of governance process through digital medium.

Besides the digital infrastructure, service delivery or use of other technological devices such as telephones, applications, and the adoption of other systems such as management information system, biometrics, smart cards, mobile, radio and television mediums for public service delivery also fall under wider perspectives of e-governance.

The E-Governance refers to the use of information technologies by government agencies to transform their relationship with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions.

B. Emergence of e-Governance Concept

The term e-Governance emerged in the late 1990s, but the history of computing in government organizations can be traced back to the beginnings of computer history. The literature on "IT in government" goes back at least to the 1970s.[50] But, mainly during the period of the last two decades, implementation of e-Governance spread out in every corner of the world and now it is considered an integral part of any development plan in both government and non-government sectors.

The United Nations (UN) started to publish the e-Government Development Index (EGDI) in 2001 which focuses on online service index, human capital index, and telecommunication infrastructure index. In the latest, the UN published its E-Government Survey in 2022 with the theme of the Future of Digital Government.[51]

In Nepal, the journey towards e-Governance can be linked to the introduction of IBM140/ System in the government

[50] Kraemer, K. L., et al. (1978). Local Government and Information Technology in the United States. Paris: OECD Informatics Studies #12.

[51] See, E-Government Survey 2022 The Future of Digital Government, UNITED NATIONS New York, 2022 https://publicadministration.un.org/en/ publicadministration.un.org/egovkb/en-us/

section in 1971. In 1996, the country established a separate Department of Science and Technology. In 2000, the Government launched its first IT Policy. Further, in association with Korea Institute of Public Administration, Nepal government launched its e-GMP (e-Governance Master Plan) in 2006. IT Policy was revised in 2010 and implemented in 2011. Similarly, Nepal Telecommunication Authority has launched its master plan for 2011-2020.[52] In 2019, the government introduced Digital Nepal Framework as a roadmap for the initiative for the digitalization of Nepal. These developments in the area of electronic governance can be summarized as the history of e-Governance in Nepal.

C. Guiding Principles and Scope of e-Governance

Throughout the world, governments are prioritizing digital technologies, data, and innovative practices, even the use of artificial intelligence in public sectors. Moreover, the private sector, going one step further massively applying digital technologies in the production and delivery of their service. As a result of it, now the public and private sector both hold massive data of citizens and businesses.

In this stage of fast-paced disruption- rapid technological evolution, changing societal needs, unexpected crisis- it is crucial to address how government can best use digital technologies and data to increase productivity and resilience in their public sector and enhance the quality of public services in an inclusive, equitable, sustainable, and trustworthy way.[53] In response to these concerns, international agencies, after considerable efforts, have created a variety of guidelines as guiding principles. The

[52] Neuro Quantology 2022; 20(10): 1142-1146

[53] OECD (2021), The E-Leaders Handbook on the Governance of Digital Government, OECD Digital Government Studies, OECD Publishing, Paris, can be accessed at https://read.oecd-ilibrary.org/governance/the-e-leaders-handbook-on-the-governance-of-digital-government_ac7f2531-en#page4

OECD highlighted three pillars and 12 recommendations on digital government strategies:

Pillar 1: Openness and Engagement:

Guiding Principles:

1. Openness, Transparency and inclusiveness,
2. Engagement and Participation in a multi-actor context in policy making and service delivery,
3. Creation of a data-driven culture
4. Protecting privacy and ensuring security

Pillar 2: Governance and Coordination

Guiding Principles:

5. Leadership and political commitment
6. Coherent use of digital technology across policy areas
7. Effective organizational and governance frameworks to coordinate
8. Strengthen international cooperation with other governments

Pillar 3: Capacities to Support Implementation

Guiding Principles

9. Development of clear business cases,
10. Reinforced institutional capacities
11. Procurement of digital technologies
12. Legal and Regulatory Framework

E-governance is not translating government into the internet but the transformation of the process through the application of digital technologies. For this, accessibility towards digital infrastructure is critical to avoid or minimize the digital divide. Similarly, a mass database of the citizen and business levels is fundamental for an effective e-governance and this level of access to data requires effective legal and regulatory framework to address the concerns of data privacy and security.

In 2002, the Center for Democracy and Technology, with the support of the World Bank, published an *E-Government Handbook For Developing Countries* which suggested the following issues to include in e-government[54], which are equally relevant in the present context too:

- providing greater access to government information;
- promoting civic engagement by enabling the public to interact with government officials;
- making government more accountable by making its operations more transparent and thus reducing the opportunities for corruption; and
- providing development opportunities, especially benefiting rural and traditionally underserved communities.

To conclude, fundamental principles of good governance such as transparency, accountability, rule of laws as well as protection of privacy and data security, access to internet, and network neutrality shall be considered as guiding principles for good e-governance.

D. Issues and Challenges

E-governance is becoming a buzzword, especially in developing countries like Nepal and major challenges are the infrastructure and accessibility.

A study conducted in 2002[55] identified seventeen challenges and opportunities in the implementation of e-governance in

[54] The Handbook can be accessed at http://www.infodev.org.

[55] Ibid 7

developing countries. Infrastructure development, law and policy framework, digital divide (literacy and accessibility), trust (privacy and security), transparency, interoperability, record management, etc. are the main challenges. These issues are still equally relevant.

The challenges in the implementation of the e-governance system identified by different research and studies in different countries such as India, Indonesia, Libya, Nepal, Mauritius, and Rwanda can be categorized as follows.[56]

1. Participation of stakeholders, Stakeholder's need assessment, Understanding the role of government
2. Traditional mindset, Proactive governance system, Understanding the needs of citizens Integrated service delivery system, Service excellence, and Enabling environment
3. Requirement of change management, Loyalty and commitments, Awareness of civil servants, Age group of civil servants, Necessary infrastructure
4. Social level, Digital divide, IT awareness Strategies and policies, Laws and legislations, Funding and business models, Infrastructure, Skilled human resources, Bureaucracy
5. Political leadership, Bureaucratic inertia, Digital divide
6. ICT infrastructure, High speed and cost-effective connectivity, Commitment and financial system, Government process, Leadership, Clear roadmap, Qualified human resources

[56] Dr. Shyan Kirat Rai, *Issues, challenges, and ways ahead to develop citizen-centric e-Governance in Nepal,* Journal of Management and Development Studies Volume: 31, Issue 1, 31-48, 2022 Nepal Administrative Staff College https://doi.org/10.3126/jmds.v31i01.52852 https://www.nasc.org.np/journals/all

7. System maturity, Business process re-engineering, Lack of integration, System scalability, Trust and awareness, Quality of data and portal, etc.

The implementation of effective e-governance faces numerous challenges, including infrastructure limitations, the digital divide, accessibility issues, policy ambiguity, and the need for a strong legal framework. Ensuring adherence to basic human rights within the e-governance system is another major challenge, encompassing concerns about data privacy and security, equitable access to digital infrastructure, and promoting inclusive participation in the e-governance process. Addressing these challenges is essential for the ethical and successful implementation of e-governance initiatives.

Chapter 11
Internet and Crime

A. Overview of Cybercrime and Its Impact on Digital Rights

Cybercrime consists of criminal acts committed online by using electronic communications networks and information systems.[57] The European Union classifies cybercrimes into three broad definitions:

- **crimes specific to the internet,** such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts);
- **online fraud and forgery**: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam, malicious code;
- **illegal online content**, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts, and glorification of violence, terrorism, racism, and xenophobia.[58]

In other words, the U.S. Department of Justice divides cybercrime into three categories:

- **crimes in which the computing device is the target -** for example, to gain network access;

[57] European Commission. (n.d.). Cybercrime.(Online materials). Available at https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en (accessed on 10 May 2024).

[58] European Commission. (n.d.). Cybercrime.(Online materials). Available at https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en (accessed on 10 May 2024).

- **crimes in which the computer is used as a weapon -** for example, to launch a denial-of-service (DoS) attack; and
- **crimes in which the computer is used as an accessory to a crime -** for example, using a computer to store illegally obtained data or digital identity theft which leads to theft of funds from a bank account.

Likewise, **Budapest Convention on Cybercrime categorizes the following:**

- Acts against the confidentiality, integrity, and availability of computer data or systems, such as Illegal access; Illegal interception; Data interference; System interference; and Misuse of devices
- Computer-related acts for personal or financial gain or harm, such as Computer-related forgery and Computer-related fraud;
- Computer content-related acts, such as offenses related to child pornography; and
- Offenses related to infringements of copyright and related rights.

It should be noted that cybercrime is motivated by various reasons, such as

- Financial Gain;
- Recognition and Achievement;
- Insider Threats;
- Political Motivations or “Hacktivism”;
- Interest of State Actors; and
- Corporate Espionage.

Some examples of cybercrimes in Nepal are presented as follows:

- The official website of the Department of Passport was hacked on June 27, 2017, by a group of Turkish hackers and defaced with threatening notes to reveal the government's data.
- On July 25, 2017, 58 government websites were reportedly hacked by a group called 'Paradox Cyber Ghost'.
- On October 23, 2017, the SWIFT system of NIC Asia Bank was reportedly hacked by an unidentified hacker. They intercepted USD 4.4 million from the utilizer accounts to six different countries.
- In March 2020, Foodmandu witnessed a data breach in their system. The hackers have leaked the database consisting of more than 50,000 Utilizer denominations, personal details, latitude, longitude, current address, emails, and phone numbers.
- In September 2020, Nepal Police apprehended five Chinese nationals who were endeavoring to withdraw cash with cloned debit cards. The alleged perpetrators had hacked the Nepal Electronic Payment System (NEPS), an interface that sanctions the transaction of money deposited in a bank by utilizing cards issued by other member banks.

Cybercrimes know no national borders i.e. criminals, victims, and technical infrastructure span multiple jurisdictions, bringing many challenges to investigations and prosecutions.[59] For instance, many types of crime, including terrorism, trafficking in human beings, child sexual abuse,

[59] Interpol.(n.d.).Cybercrime. .(Online materials). Available at https://www.interpol.int/en/Crimes/Cybercrime (accessed on 10 May 2024).

and drug trafficking, hasmoved online or are facilitated online.[60]

Cybercrime have a chilling effect on the digital rights of individuals in several ways:

- **Privacy Violations:** Data breaches and hacking expose personal information, violating our right to privacy.
- **Restrictions on online freedom of expression:** The government may restrict legitimate expression while combating misinformation, disinformation, and fake news.
- **Silencing Dissent:** Cyberbullying and harassment can intimidate individuals from expressing their opinions freely online.
- **Surveillance and Censorship Tools:** Governments may exploit cybercrime concerns to justify surveillance programs and content restrictions, hindering freedom of expression.
- **Self-censorship:** Fear of cyber attacks can lead individuals and organizations to self-censor or avoid expressing controversial viewpoints.
- **Trust Deficit:** Widespread cybercrime can erode trust in online platforms and discourage participation in the digital space.

B. Legal Responses to Cybercrime

As aforementioned, Cybercrime poses a significant threat, not just to financial security but also to digital rights. Responding to and combating cybercrimes requires clear national legislation such as:

[60] European Commission. (n.d.). Cybercrime.(Online materials). Available at https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en (accessed on 10 May 2024).

- **Cybercrime Laws:** Most countries have enacted specific legislation to address cybercrimes like hacking, data breaches, and cyber fraud. These laws clearly define criminal offenses, establish proportionate penalties, and empower law enforcement to investigate and prosecute cybercriminals. For instance, in the United States of America, the Computer Fraud and Abuse Act (CFAA), enacted in 1986 prohibits unauthorized access to computer systems and hacking.
- **Data Protection Laws:** Regulations like the European Union's General Data Protection Regulation (GDPR) aim to protect personal data privacy and security. These laws hold companies accountable for data breaches and empower individuals to control their personal information online. They also serve as a legal tool for victims of cybercrime to seek compensation for damages.

For instance, in Nepal, there is no clear legislation that criminalizes cybercrime. Laws are indeed scattered and fragmented. Equally, it should be noted that cybercriminals are constantly developing new techniques and exploiting vulnerabilities. Therefore, legal frameworks and enforcement strategies need to be adaptable to keep pace with these changes, through revising existing laws and incorporating emerging threats into the legal definition of cybercrime.

Key legislations related to cybercrimes in Nepal are as follows:

- **Electronic Transactions Act, 2006, and Electronic Transaction Rule in 2008**

Section 47 of the Act prohibits the **publication of illegal materials in electronic form. Sub-section (1)** states that if any person publishes or displays any material in electronic media including computer, internet which is prohibited to the publish or display by the prevailing law or which may be contrary to the public morality or decent behavior or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities shall be liable to the punishment with the fine not exceeding One Hundred Thousand Rupees or with the imprisonment not exceeding five years or with both.[61] This Section has been widely used to prosecute cybercrimes in Nepal.

- **National Penal Code, 2018**

  Provisions like Section 121 of the Code can be used to prosecute cybercrimes relating to producing or selling obscene books, pamphlets, etc. This may be misused to limit the freedom of expression online. Any person committing this offense is liable to a sentence of imprisonment for a term not exceeding one year or a fine not exceeding ten thousand rupees or both sentences.

- **Individual Privacy Act, 2018:** Privacy is a constitutional right in Nepal. Section 19 of the Act ensures online privacy. Under this Act, every person has the right to privacy in the matters related to their personal information, a written instrument, correspondence, statistics, or character stored on the electronic means.[62] It also protects that no one shall get unauthorized access to a person's information, notice, or correspondence stored on electronic means, violate their privacy or make them accessible to anyone. This Act makes a provision of express consent. The personal

[61] Section 47, *Electronic Transaction Act, 2006.*

[62] Section 19, *The Privacy Act, 2018.*

information collected by a public body or the personal information under the control of or holding of such a body shall not be used or given to anyone without the consent of the concerned person.[63]

It should be noted that the Nepal Police has a Cyber Bureau dedicated to tackling cybercrime in Nepal.[64] The Cyber Bureau is a specialized unit within the Nepal Police that focuses on investigating and prosecuting cybercrimes.[65] The Bureau is located in Kathmandu and has started accepting complaints through phone and email.

C. Collaboration and Cooperation in Combating Cybercrime

The United Nations Office on Drugs and Crimes rightly points out that combating cybercrime and protecting our digital rights requires a collaborative effort from various actors and stakeholders at national, regional, and international levels.[66] Combating cybercrime necessitates ongoing improvements in legal frameworks, international cooperation, and collaboration between governments, law enforcement agencies, tech companies, and civil society.[67]

- **International cooperation (through adopting treaties and conventions and international institutional**

[63] Section 26, *The Privacy Act, 2018.*

[64] Cyber Bureau (online material). Available at https://www.nepalpolice.gov.np/other_links/detail/cyber-bureau/ (accessed on 8 May 2024).

[65] Cyber Bureau (online material). Available at https://www.nepalpolice.gov.np/other_links/detail/cyber-bureau/ (accessed on 8 May 2024).

[66] UNODC. (n.d.). Cybercrimes. (online material). Available at https://www.unodc.org/westandcentralafrica/en/index.html (accessed on 7 May 2024).

[67] Interpol.(n.d.).Cybercrime. .(Online materials). Available at https://www.interpol.int/en/Crimes/Cybercrime (accessed on 10 May 2024).

mechanisms): International agreements like the Budapest Convention on Cybercrime form the cornerstone of global cooperation. These treaties establish a framework for information sharing, evidence gathering, and extradition. This allows nations to jointly investigate and prosecute cybercriminals who operate across borders. This treaty is a regional treaty and the United Nations has yet to adopt an international treaty in this regard. Likewise, organizations like Interpol and Europol play a vital role in coordinating international efforts to combat cybercrimes. They facilitate the exchange of intelligence, provide technical assistance to member states, and help conduct joint investigations.

- **Governments:** Governments need to develop effective cybercrime legislation while upholding human rights principles.
- **Law Enforcement Agencies:** Law Enforcement agencies need to prevent and investigate cybercrimes effectively. They should be able to collect digital forensics as well.[68]
- **Tech Companies:** Tech companies have a responsibility to improve cyber security measures and promote responsible content moderation practices.
- **Individuals:** Individuals should be educated on cyber threats and best practices for online safety. They should have enhanced capacities and a high level of digital literacy to protect and be safe from cybercrimes. They should focus on maintaining digital hygiene and economic digital footprints.

[68] UNODC. (n.d.). Cybercrimes Modules. (online material). Available at https://www.unodc.org/westandcentralafrica/en/index.html (accessed on 7 May 2024).

- **Civil Society Organizations:** Civil Society Organizations play a crucial role in advocating for digital rights and holding governments and companies accountable.

Chapter 12

Support/Grievance Mechanisms to address online violence

A. Importance of Support and Grievance Mechanisms

As online interaction and digital services are prevalent, support and grievance mechanisms play a crucial role in ensuring a safe, fair, and healthy digital environment for users.[69] Generally, reporting content to digital platforms requires a user to describe the incident and type of threat that has occurred, whether it's sexual, exploitative, violent, physically threatening, etc.[70] Platforms, like Twitter and Facebook, have "flagging" options built directly into the interface, giving users the option to report content the moment they see it.[71] It has become more and more easy to report content and grievances relating to online platforms.

- **Social Media Platforms:** Most social media platforms have reporting mechanisms for users to report and flag abusive content or behavior.

[69] Online Harassment Field Manual. (Online material). Available at https://onlineharassmentfieldmanual.pen.org/reporting-online-harassment-to-platforms/ (Accessed on 9 May 2024).

[70] Online Harassment Field Manual. (Online material). Available at https://onlineharassmentfieldmanual.pen.org/reporting-online-harassment-to-platforms/ (Accessed on 9 May 2024).

[71] Online Harassment Field Manual. (Online material). Available at https://onlineharassmentfieldmanual.pen.org/reporting-online-harassment-to-platforms/ (Accessed on 9 May 2024).

- **E-commerce Websites:** E-commerce platforms typically have customer support options to address issues with purchases, returns, or product information.
- **Government Websites:** Many government websites offer online complaint mechanisms for citizens to report grievances related to public services.

The significance and importance of support and grievance mechanisms are presented as follows:

- Grievance mechanisms protect users from online abuse and harassment. Grievance mechanisms allow users to report incidents of online abuse, harassment, or bullying. This empowers users to take control of their online experience and hold others accountable for their actions.
- Support and grievance mechanisms help users resolve issues with online services or platforms. This could include problems with billing, account access, technical difficulties, or content moderation decisions.
- By providing avenues for reporting harmful content like hate speech or misinformation, these mechanisms contribute to a safer online environment for everyone.
- Having clear and accessible grievance procedures shows users that a platform or organization takes their concerns seriously. This fosters trust and transparency in the online environment.
- Grievance mechanisms provide a way for users to hold platforms accountable for their policies and how they enforce them. This can lead to improvements in content moderation and user protection measures.
- Knowing that there are consequences for inappropriate behavior can deter users from engaging in online harassment or spreading misinformation.

B. Role of Civil Society and Advocacy Groups

Civil society organizations and advocacy groups play a critical role in supporting and strengthening grievance mechanisms, ensuring they function effectively and protect user rights.

- **Raising Awareness and digital literacy:** CSOs and advocacy group can educate users about their rights online and how to utilize existing grievance mechanisms. This can be done through workshops, online campaigns, and informational resources.
- **Watch dog (Monitoring and Evaluation):** CSOs and advocacy can monitor how grievance mechanisms are functioning, analyzing their accessibility, responsiveness, and fairness. This helps identify areas for improvement. This leads to greater transparency from platforms and governments regarding the handling of user grievances. This includes publishing data on the number and types of complaints received and the actions taken.
- **Empowering Users as right holders:** Some CSOs and advocacy group offer legal aid and support to users who face challenges in navigating grievance procedures or seeking legal recourse for online harms. They can create online communities or forums where users can share their experiences with grievance mechanisms and support each other. Likewise, CSOs and advocacy groups play a crucial role in referral system by linking services needed to users and organizations offering such services.
- **Engaging with multi-stakeholders:** CSOs and advocacy groups can act as facilitators between users, platforms, and governments, promoting constructive dialogue on how to improve grievance mechanisms and

address online harms. They can build pressure on multiple stakeholders who are duty bearers to address and resolve grievances.

- **Policy Advocacy:** CSOs and advocacy groups can lobby policymakers to enact legislation or regulations that require robust grievance mechanisms for online platforms and services.

C. Governmental and Non-Governmental Support Services

Governmental Support:

- **Cyber Bureau of Nepal Police:**

  Nepal Police has a Cyber Bureau, a specialized unit within the Nepal Police that focuses on investigating and prosecuting cybercrimes.[72] The Bureau is located in Kathmandu and has started accepting complaints through phone and email.

- **National Telecom Authority (NTA):**

  The NTA is responsible for regulating the telecommunications sector in Nepal. Users can file a complaint with the NTA if a telecommunications service provider is not addressing concerns about abusive content or hateful content.

Non-Governmental Organizations:

- **Legal Aid Organizations:**

  CSOs providing legal aid may assist with filing complaints related to online harassment or privacy violations. For instance, legal aid provided by the Nepal Bar Association

[72] Cyber Bureau (online material). Available at https://www.nepalpolice.gov.np/other_links/detail/cyber-bureau/ (accessed on 8 May 2024).

- **Digital Rights Advocacy Groups:**

  Organizations like Digital Rights Nepal can support advocacy for ensuring digital rights and may offer resources or guidance on handling online grievances.

Useful Hotlines

- **National Emergency Hotline Number 100:** This hotline can be used to report the crime.
- **Child Hotline Number 1098:** The child hotline number 1098 is a reliable resource for children facing abuse, neglect, or other challenges.[73]
- **National Women Commission's Hotline Number 1145**: This hotline provides critical support to women facing various issues.[74]

[73] https://cwin.org.np/programs/child-protection-and-helpline/#:~:text=%E2%80%93%20Collection%20and%20dissemination%20of%20information,relief%2C%20and%20protection%20for%20children (accessed on 10 May 2024).

[74] https://nwc.gov.np/en/ (accessed on 10 May 2024).

Chapter 13

Digital Wellbeing

Digital well-being refers to the impact of technology on our mental, physical, and emotional health. It involves practices that balance online and offline activities, such as managing screen time, setting boundaries with technology, and being mindful of digital consumption. It aims to ensure healthy and productive use of technology. For employees, this means promoting habits that support physical and mental health. Digital wellness includes both disconnecting from devices and considering how technology affects overall well-being.

A. Impacts of Digital Technologies in Wellbeing

1. **Physical Health**: Many technology-based activities, such as using computers, smartphones, tablets, and gaming consoles, involve prolonged periods of sitting or sedentary behavior. This sedentary lifestyle can lead to a decrease in physical movement and contribute to a lack of exercise.

2. **Screen Time**: Excessive screen time, whether for work, entertainment, or socializing, can displace time that could be spent engaging in physical activities such as exercise, sports, or outdoor play. The more time individuals spend on screens, the less time they may allocate to physical movement and exercise.

3. **Indoor Engagement**: Technology often promotes indoor sedentary activities, which can deter individuals from participating in outdoor physical activities or exercise. The convenience and entertainment value of

technology may lead individuals to choose screen-based activities over physical pursuits.

4. **Social Interaction**: Virtual social interactions facilitated by technology, such as social media, online gaming, and video calls, can replace face-to-face social engagements and physical activities. Spending time on digital platforms may reduce opportunities for physical social interactions that involve movement and exercise.

5. **Impact on Health**: A lack of physical exercise due to technology use can contribute to various health issues, including obesity, cardiovascular problems, musculoskeletal disorders, and decreased fitness levels. Regular physical activity is essential for maintaining a healthy weight, improving cardiovascular health, and enhancing overall physical well-being.

B. Strategies for Promoting Digital Wellbeing

It is essential to understand that the value of technology depends on how it is used, by whom, when, and for what purpose. Technology itself is not inherently good or bad; its impact varies based on its application. Identifying and reducing the most significant risks to well-being from using digital technology is crucial. This involves understanding the potential dangers and finding ways to mitigate them.

To address the impact of technology on physical health, individuals are encouraged to adopt strategies that promote a balance between technology use and physical activity. This may include setting limits on screen time, incorporating physical exercise into daily routines, engaging in outdoor activities, participating in sports or fitness classes, and prioritizing movement and exercise for overall physical health and well-being. Balancing technology use with physical activity is crucial for maintaining a healthy lifestyle and reducing the negative effects of sedentary behavior on physical health.

Take Breaks and Schedule Tech-Free Time: We need to incorporate breaks throughout our day where we consciously step away from all digital devices. Plan these breaks in advance, like taking a walk during your lunch break, setting aside an hour before dinner for device-free conversation with family, or taking some time for physical exercise.

Switch Off Distractions and Prioritize Real-Life Interactions: When we are using technology, we can silence notifications and focus on the task at hand. This will help in being more present at the work being carried out and be more productive. Instead of scrolling through social media while catching up with friends and families we can just put away the phone and focus on the conversation and real-life interactions.

Practice Digital Detox: While taking breaks are general norms, a digital detox is even more essential, it is a more extended period of disconnecting from technology. This could be a few hours, a whole day, or even a weekend. It allows us to reset our relationship with tech and refocus on real-world experiences, nature, and family time.

Turn Off All Screens an Hour Before Bedtime: We might not be aware but the screens of our digital gadgets emit blue light which can disrupt the sleep cycle. To avoid this we need to develop a habit of powering down devices well before bedtime, it'll give your brain time to wind down and prepare for sleep.

Use Digital Wellbeing Apps: Digital tools are also handy ways that can help maintain our digital well-being. Many smartphones and tablets come with built-in digital wellbeing features. These tools can track screen time, app usage, and set limits on notifications and device use.

Seek Help if Needed: It is not always the same case and some people might be struggling with anxiety, depression, or feelings of inadequacy due to social media, and if you find yourself in such a situation don't hesitate to seek help from a professional. A therapist can offer guidance on developing healthy online habits and managing your relationship with social media and your digital presence.

C. Support Services Available for Digital Wellbeing

In this chapter we will discuss the available support mechanism that could be explored to maintain the digital wellbeing of an individual and family.

Online Communities and Forums: Platforms where individuals can connect with others facing similar challenges related to digital wellbeing, share experiences, seek advice, and provide support to one another.

Counseling and Therapy Services: Professional counseling services that specialize in addressing issues related to digital addiction, screen time management, and overall digital wellbeing through individual or group therapy sessions.

Digital Detox Retreats: Retreats or programs designed to help individuals disconnect from digital devices, engage in offline activities, practice mindfulness, and reset their relationship with technology for improved mental and emotional wellbeing.

Educational Workshops and Seminars: Events and workshops focused on educating individuals about the impact of excessive screen time, providing strategies for managing digital usage, and promoting healthy technology habits for better overall wellbeing.

Mobile Applications and Tools: Digital wellbeing applications and tools, such as those mentioned earlier, that offer features for tracking screen time, setting usage limits, providing insights into digital habits, and encouraging healthier device usage.

Employee Assistance Programs (EAP): Workplace programs that may include resources and support for employees dealing with digital addiction, stress related to technology use, and strategies for maintaining a healthy work-life-tech balance.

Telehealth Services: Remote healthcare services that offer digital wellbeing support through virtual consultations, therapy sessions, and resources for managing screen time and promoting healthy technology habits.

D. Digital Tools for Digital Wellbeing

We have already discussed the importance of wellbeing in the digital age and the consequences. Now we will discuss Digital tools that can promote wellbeing in the digital age. These tools are invaluable in helping individuals, families and organizations maintain a healthy balance between digital engagement and overall health. Utilization of these tools, you can enhance productivity, improve mental and physical health, and foster a more balanced digital life. Here are the list of digital wellbeing apps that are beneficial for individual, family and organizational purpose:

SPACE Break Phone Addiction:

This app Provides insights into users' digital usage patterns, tracks screen time, sets goals for phone usage, offers reminders to take breaks, and encourages healthier smartphone habits.

Google Digital Wellbeing (GDW):

Helps users understand their digital habits through detailed usage statistics, allows users to set daily limits on app usage, includes a Wind Down feature to reduce screen time before bed, provides app timers to limit usage, and offers a Do Not Disturb mode.

NUGU:

It promotes healthier technology usage habits by tracking screen time, providing notifications for excessive usage, offering insights into app usage patterns, and encouraging breaks from digital devices.

FamiLync:

Focuses on family digital wellbeing by allowing parents to monitor and manage screen time for children, set usage limits, track device usage, and promote healthy digital habits within the family.

MyTime:

Assists users in managing screen time by tracking usage patterns, setting goals for device usage, providing insights into app usage, and encouraging breaks from digital devices to maintain a healthy balance.

Lock n'LoL:

Helps users manage screen time and reduce distractions by allowing them to lock certain apps or functions for a specified period, set time limits for app usage, and customize restrictions to promote focused and mindful device usage.

Apple's Screen Time:

Enables users to monitor their screen time, set app limits for specific categories or individual apps, schedule downtime to disconnect from devices, view activity reports to understand usage patterns, and set parental controls for family members.

UNITED STATES EMBASSY

2024 ALUMNI ENGAGEMENT INNOVATION FUND

Digital Rights Nepal

NUSAN Nepal- US Alumni Network

Digital Rights and Safety Handbook is part of the Nepal Digital Rights School, run by Digital Rights Nepal, in Collaboration with Nepal US Alumni Network, with the support of US Embassy in Kathmandu under Alumni Engagement Innovation Fund 2023.

Digital Rights
Nepal

Phone	+977 9767245100
Address	47-Neel Saraswoti Marga, Gairidhara-2, Kathmandu
Email	info@digitalrightsnepal.org.np
Web	www.digitalrightsnepal.org

For more info: www.digitalrightsnepal.org @digitalrightsNP